



GUIDEBOOK

on security measures
for religious sites & communities



This project is funded by the European Union's
Internal Security Fund – Police under Grant
Agreement No. 101034230 – ProSPeReS

prosperes.eu

The ProSPeReS Consortium

Security experts, security research and academic institutions,
providers of technical solutions and services



Law enforcement agencies (LEAs)



Faith-based organizations



Document description

WP number and title	WP3 – Preparing tailor-made security measures for religious sites. D.3.3 – A guidebook including recommendations for procedures, equipment and templates to prevent, protect, detect, respond to and mitigate the result of a terrorist attack.
Lead Beneficiary/Author(s)	UL (Michał Stachyra, Rafał Batkowski)
Contributor(s)/Author(s)	UL, DSC, ISEMI, WSB, DISSS, HELLENBERG, CARDET, Archdiocese, Lodz, Social Obser., HMI, GWZ Warsaw, KWP Lodz, KSP, KWP Wroclaw, HELLENIC POLICE, CBK PAN, SGSP
Document type	Report
Last Update	06.03.2023 by UŁ
Dissemination level	Public / Confidential *

* Confidential – only for members of the consortium & EC Services

Acknowledgement:

This project is funded by the European Union's Internal Security Fund — Police. Grant Agreement No. 101034230 — ProSPeReS

Disclaimer:

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



This work is licensed under the Creative Commons Attribution 4.0 International Licence. To view a copy of this license, visit creativecommons.org/licenses/by/4.0/ with relevant national copyright provisions to be applied accordingly.

The material for this publication was developed and reviewed by the ProSPeReS consortium:

No	Partner organisation name	Short Name	Country
1	UNIVERSITY OF LODZ	UL	PL
2	DYNAMIC SAFETY CORPORATION	DSC	PL
3	INTERNATIONAL SECURITY AND EMERGENCY MANAGEMENT INSTITUTE	ISEMI	SK
4	CENTRE FOR SECURITY STUDIES	KEMEA	GR
5	WSB ACADEMY	WSB	PL
6	STICHTING DUTCH INSTITUTE FOR SAFE AND SECURE SPACES	DISSS	NL
7	HELLENBERG INTERNATIONAL	HELLENBERG	FI
8	CENTRE FOR THE ADVANCEMENT OF RESEARCH & DEVELOPMENT IN EDUCATIONAL TECHNOLOGY LIMITED	CARDET	CY
9	ARCHDIOCESE OF LODZ	Archdiocese Lodz	PL
10	SOCIAL OBSERVATORY FOUNDATION	Social Obser.	PL
11	HOLY METROPOLIS OF IOANNINA	HMI	GR
12	JEWISH COMMUNITY OF WARSAW	GWZ Warsaw	PL
13	LODZ VOIVODESHIP POLICE	KWP Lodz	PL
14	WARSAW METROPOLITAN POLICE	KSP	PL
15	WROCLAW VOIVODESHIP POLICE	KWP Wroclaw	PL
16	HELLENIC POLICE	HP	GR
17	SPACE RESEARCH CENTRE POLISH ACADEMY OF SCIENCE	CBK PAN	PL
18	THE MAIN SCHOOL OF FIRE SERVICE	SGSP	PL

Table of Contents

Abbreviations	6
Definitions	8
1. Executive summary.....	10
2. Introduction	12
2.1. EU security environment regarding public places and religious sites.....	13
2.2. General information about the ProSPeReS project	19
2.2.1 WP3 objectives.....	21
2.3. Results of ProSPeReS workshops and case studies regarding various places of worship...22	
3. Multi-stakeholder and community cooperation	27
3.1. Introduction to the cooperation	27
3.2. Definitions and theory	28
3.3. Tips for good communication.....	32
3.4. Suggestions on how to build and manage multi-stakeholder and community cooperation ...33	
3.5. Summary 3.2.- 3.4.	36
4. Recommendations	39
4.1. Prevention.....	40
4.2. Protection.....	52
4.3. Detection.....	56
4.4. Response.....	59
4.5. Mitigation of the results of terrorist attacks	60
5. General idea of awareness and training	64
6. Conclusions	67
7. List of tables, figures and pictures	70
8. List of appendices	72
9. References.....	73

Abbreviations

Table 1 – Abbreviations used in the document

Acronyms / Abbreviations	Description
BWA	<i>Blade Weapon Attack</i>
CBR	<i>Chemical, Biological, Radiological (agents)</i>
CBRN-E	<i>Chemical, Biological, Radiological, Nuclear, Explosive (substances and agents)</i>
CCTV	<i>Closed Circuit Television</i>
COMECE	<i>Commission of the Bishops' Conferences of the European Union</i>
CPTED	<i>Crime Prevention Through Environmental Design</i>
DG HOME	<i>Directorate-General for Migration and Home Affairs</i>
EC	<i>European Commission</i>
EOD	<i>Explosive Ordnance Disposal</i>
ETA	<i>Estimated Time of Arrival</i>
EU	<i>European Union</i>
FAA	<i>Firearms Attack</i>
GTI	<i>Global Terrorism Index</i>
HE	<i>High Explosive</i>
IED	<i>Improvised Explosive Device</i>

ISFP	<i>Internal Security Fund Police</i>
LEAs	<i>Law Enforcement Agencies / Agents</i>
PBIED	<i>Person-Borne Improvised Explosive Device</i>
ProSPeReS	<i>Protection System for large gatherings of People at Religious Sites</i>
PSOI	<i>Public Space of Interest</i>
PW	<i>Place of Worship</i>
RSOOI	<i>Religious Site of Interest</i>
SOF	<i>Special Operations Forces</i>
SOI	<i>Site of Interest</i>
UAV	<i>Unmanned Aerial Vehicle</i>
UAVIED	<i>Unmanned Aerial Vehicle (borne) Improvised Explosive Device</i>
VA	<i>Vulnerability Assessment</i>
VAC	<i>Vulnerability Assessment Checklist</i>
VAT	<i>Vulnerability Assessment Tool</i>
VBIED	<i>Vehicle-Borne Improvised Explosive Device</i>
VWA	<i>Vehicle Weapon Attack</i>
WP	<i>Work Package</i>
WTMD	<i>Walkthrough Metal Detector</i>

Definitions

Table 2 – Definitions used in the document

Terms	Description
capability	<i>A demonstrable ability to respond to, and recover from, a particular threat or hazard</i>
command and control	<i>The exercise of authority using communications and the management of available assets and capabilities to achieve defined objectives</i>
contamination	<i>The unintended or undesirable presence or transfer of hazardous chemical, biological or radiological (CBR) substances/materials to people, objects, soil or water</i>
decontamination	<i>The removal or reduction of hazardous materials to lower the risk of further harm and/or cross contamination</i>
ETHANE	<i>A structured report to provide key information needed by the emergency services during an emergency (Exact location / Type of incident / Hazards / Access / Number of casualties / Emergency services)</i>
exercise	<i>A simulation designed to validate a capability to manage incidents and emergencies. Specifically, exercises will seek to validate training undertaken and the procedures and systems within emergency or business continuity plans (but are not a substitute for training)</i>
evacuation	<i>Movement of people from a place of actual or potential danger to a safer place to reduce their risk of harm</i>
forward command post	<i>A command-and-control facility nearest to the scene of an incident responsible for the immediate deployment and direction of resources (may be a single or multi-agency facility)</i>
hazard	<i>A substance, object, situation or behaviour that has the potential to cause harm to people or property</i>
incident manager	<i>The person with overall responsibility and authority for decisions and resources during an emergency at the place of worship or large religious gathering</i>
interoperability	<i>The extent to which organisations can work together efficiently and effectively as a matter of routine</i>

invacuation	<i>Movement of people inside a building or structure from a place of actual or potential danger to reduce their risk of harm</i>
lockdown	<i>The process of securing a building/site to prevent to keep a threat or attack outside (or delay/frustrate entry) and protect people and property inside. A 'lockdown' can be full, partial, zonal or phased depending on the circumstances of the threat/attack</i>
mass decontamination	<i>The physical process of rapidly removing contaminants form a large number of people at the same time, in potentially life-threatening situations to lower the risk of further harm and/or cross contamination</i>
police	<i>Term police in this meaning represents also other LEAs across EU, (e.g., Gendarmerie, Carabinieri etc.)</i>
protected space	<i>A location inside a building that has been developed/adapted for sheltering people from a threat or attack</i>
rendezvous point	<i>The place where emergency services (personnel, vehicles, equipment) for briefing and deployment to an incident (may be a single or multi-agency facility)</i>
safe room	<i>A room specifically designed and constructed for sheltering people from a threat or attack within a building</i>
threat	<i>An expression of intention to inflict evil, injury, or damage</i>
threat assessment	<i>Threat assessment is the practice of determining the credibility and seriousness of a potential threat, as well as the probability that the threat will become a reality.</i>
triage	<i>The first assessment of patients or casualties to determine the urgency of their need for treatment and the nature of treatment required</i>
vulnerability	<i>The quality of being vulnerable (= able to be easily hurt, influenced, or attacked)</i>
vulnerability assessment	<i>A vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system</i>
welcome team	<i>A team with responsibility for welcoming worshippers and visitors at large gatherings and events who are trained and exercised in security and emergency procedures to provide an increased and improved capability for the place of worship in detecting, deterring and delaying general security threats - including terrorist/extremist threats and attacks</i>

1. Executive summary

The ProSPeReS project, dedicated to the security of places of worship, in particular the protection of worshippers, involves the work of experts, police officers and officials, firefighters, scientists, and representatives of various religious communities.

The '*Guidebook on security measures for religious sites and communities*' is an integral component of the joint expert work of the consortium led by the University of Lodz.

Recommendations based on analyses, research projects and workshops have made it possible to compile a single guide covering, among others, the following items:

- procedures related to preventing a terrorist threat, and reacting after a threat has been identified;
- the Security by Design concept addressed towards places of worship;
- review of available technical security equipment and personal protective equipment to be used as part of strengthening the resilience of places of worship;
- communication protocols between places of worship staff and other entities involved in protecting places of worship and reacting in the face of an attack;
- specific, simple tools and tips for places of worship security, e.g.: Vulnerability Assessment Tool LITE version and Checklist for systemic care of places of worship security.

The recommended solutions and security concepts were thoroughly discussed with representatives of Christian, Jewish and Muslim communities, and the authors are convinced of their practicality and value and moreover, that they can be directly applied by administrators of places of worship and organisers of faith-based events.

The main goal of the Guidebook is to provide a set of procedures, solutions, and recommendations that will strengthen the resilience of places of worship in dealing with terrorist threats. In order to identify such threats and address the challenges of organizing major religious events, striving for better cooperation within the local security environment and establishing close relationships with local authorities, LEAs, fire services and neighbours are all strongly recommended.

The content of the Guidebook is addressed to people interested in increasing the level of security of places of worship but who have neither the education nor the experience related to security or law enforcement. Taking this into consideration, the authors tried to make the guidebook as simple and easy to understand as possible for the user. Guidebook Users will find links and QR-codes that refer them to relevant content and materials developed for the ProSPeReS project.

Please familiarize yourself with the Guidebook. Adopting a consistent, comprehensive approach will enable you to improve the security of your places of worship.

The '*Guidebook on security measures for religious sites and communities*' lays out a set of procedures for preventing, protecting, detecting, responding to, and mitigating the effects of terrorist attacks. Its aim is to emphasize the basic assumption of the project - to develop a simple and universal guide, the implementation of which will not require large financial and organisational expenses, and whose implemented solutions can effectively minimize the risk of a terrorist attack.

Chapter 2 introduces the user to the basics of the EU security environment for public and religious places. It defines places of worship and shows data on terrorist threats in the EU. Also, in this chapter, the user has the opportunity to become acquainted with the ProSPeReS project and the results of ProSPeReS workshops and case studies on various places of worship.

In Chapter 3, the user is presented with information on how to build communication and cooperation with local communities and individual interested persons.

The authors provide the user with useful definitions and explain why establishing good communication between multiple stakeholders and good community collaboration is vital for ensuring the safety of religious sites. At the end of the chapter, there are suggestions about ways to build and manage multi-stakeholder and community cooperation.

Chapter 4 proposes adopting more consistent approaches to safeguarding the faithful in places of worship.

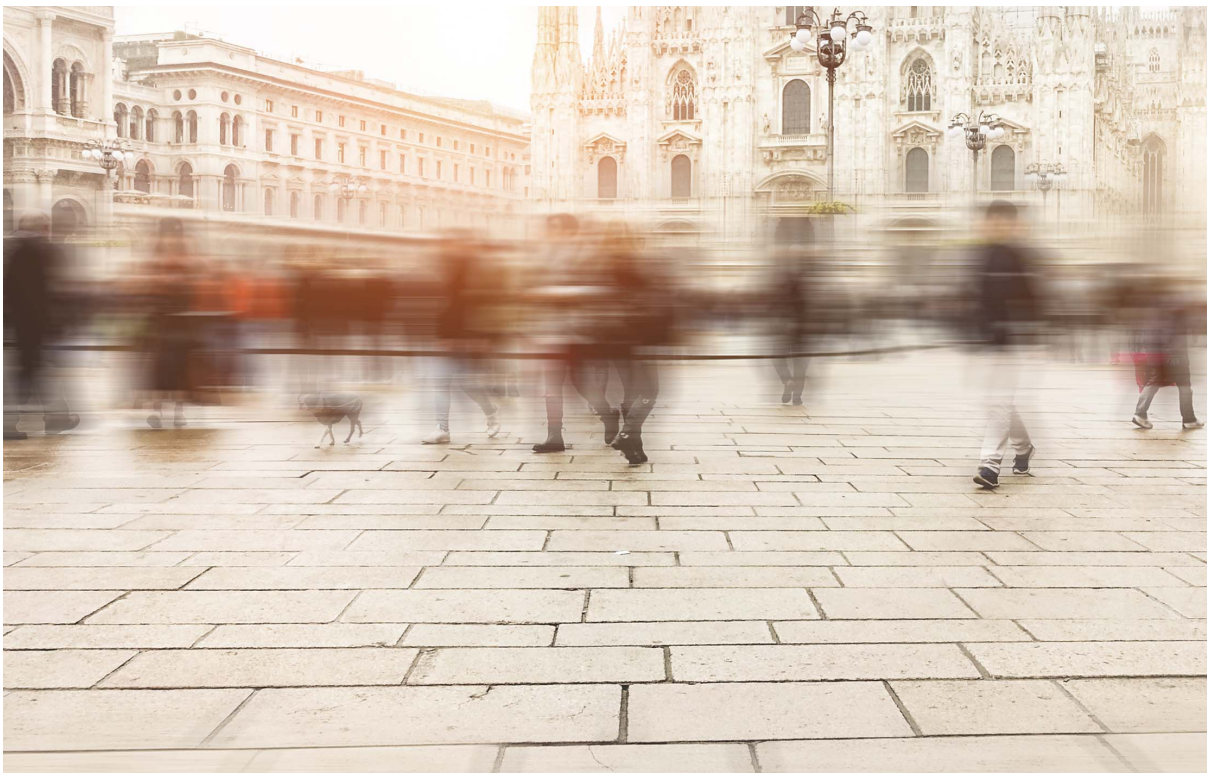
The chapter helps the user find the essential elements related to the topics in question: prevention, protection, detection, response and mitigation, which are contained in the appendices attached to the Guide - QR-codes and links listed above.

Chapter 5 outlines training option for users.

Chapter 6 contains the Guidebook summary.

Relevant deliverables are included in the Guidebook Appendices. Please familiarize yourself with the Appendix.

Picture 1 – Gathering by a place of worship



2. Introduction

The fundamental aim of the policies and activities implemented within the European Union is to protect the residents of EU Member States from serious threats, including those categorized as terrorism at both the national and Union level.

The EU Counter-Terrorism Agenda, which is related to the EU Security Union Strategy 2020-2025, is a framework for building the resilience of societies against radicalization, violent extremism, and terrorism. The proposed activities on the Agenda shown in the graph below affect many aspects of our lives, and also apply to places of worship and religious communities.

Figure 1 – Actions based on the EU Counter Terrorism Agenda



Source: European Commission (2020). *Counter Terrorism Agenda*¹.

The ProSPeReS project corresponds to steps taken in the EU to counteract serious threats, with a particular focus on terrorism. This Guidebook, which is primarily directed at religious communities, is a collection of recommendations developed by experts, scientists, LEAs, Fire Service and representatives of religious communities, including those managing places of worship. This Guidebook is being made available in the hope that the proposed good practices and recommendations contained in it we hope

¹ European Commission (2020). *Counter Terrorism Agenda*. Retrieved on June 19th, 2021. URL: https://ec.europa.eu/home-affairs/sites/default/files/what-we-do/policies/european-agenda-security/20201209_counter-terrorism-agenda-eu_en.pdf

that it sufficiently cover your needs and requirements and be applied in your churches, mosques, and synagogues.

2.1. EU security environment regarding public places and religious sites

To begin with, the authors of the guidebook would like to systematize the selected information and definitions that will be used later in the publication to discuss public spaces and places of worship inside the European Union in the context of a security environment.

Public spaces, namely, crowded public places² including the metro, shopping centres, sports stadiums, bars, restaurants, clubs and commercial sidewalks are easily accessible to the public, but also an easy target for terrorists to do great harm³. Public spaces categories present soft target characteristics:

Table 3 – Public spaces categories presenting soft target characteristics. D 2.1 - Manual for vulnerability assessment

Category	Examples
Transport hubs	<i>Train stations, bus hubs, underground metro stations, etc.</i>
Squares	<i>Public squares, where many events take place are next to important buildings, and have regular big markets, festivals, etc.</i>
Shopping areas	<i>Shopping malls, main shopping streets in the city centre, etc.</i>
Nightlife areas	<i>Areas with a high density of bars, pubs and/or nightclubs, restaurants, coffee shops, small concert halls, etc.</i>
Cultural venues	<i>Concert halls, museums, monuments, sport events, stadiums, amusement parks, tourist sites, etc.</i>
Business venues	<i>Big hotels with meeting rooms, large offices, conference centres, etc.</i>
Places of worship (PW)	<i>Churches, mosques, synagogues, etc.</i>
Institutional venues	<i>Governmental / municipal buildings, health buildings, educational buildings, etc.</i>

² The European Union (EU) Action plan to support protection of public spaces. p.2. Retrieved on July 20th, 2022. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0612>. .

³ ProTECT project (2021). *Deliverable 2.1. Manual EU VAT*, p. 8-10. Retrieved on July 20th, 2022. URL: https://protect-cities.eu/wp-content/uploads/2021/02/PRoTECT_Deliverable-2.1-Manual-EU-VAT_v2.0.pdf.

Soft targets are places⁴ that support community and economic prosperity, where people congregate to study, shop, dine, conduct business, are entertained, worship, or travel. In general, because they must be open and accessible to the public, they have little or no security.

A religious site, a place of worship - refers to any temple, shrine, site, faith community centre or religious school where worship of any religion is practiced. The basic principles to follow when designing tailor-made protection solutions for a particular place of worship are similar to techniques employed for other public spaces deemed to be soft targets: threat identification and assessment, vulnerability assessment, likelihood/consequences evaluation, selection of counter/mitigation measures as well as rehearsal and review of security planning⁵. Additionally, recommendations encompass the correct procedures to manage risks and mitigate threats against large gatherings of worshippers.

Places of worship are categorized as public spaces and are soft targets.

Why do the European Commission and the competent institutions of the EU Member States deal with the security of public places and places of worship? Unfortunately, public places, including places of worship and people located there, have often been the target of terrorist organisations, individual terrorists and armed criminals⁶.

Examples of terrorist attacks in the EU in recent years (Paris, London, Manchester, Stockholm, Copenhagen, Berlin, Brussels, Barcelona) show unequivocally that they were aimed at public places that were a typical soft target. Terrorism has for decades been a reality in many European countries and a constant threat to a great number of European citizens. The most lethal form of terrorism in the EU over the past decade has been religious terrorism. Islamic terrorist groups or lone actors inspired by jihadist groups have been responsible for 528 deaths due to terrorism in the West since 2007. The most noticeable surge in Islamic terrorism in the West was between 2015 and 2017, with 63 attacks and 457 deaths in 11 countries⁷. It seriously threatens the security, values of democratic states, and the rights and freedoms of citizens. Acts of terrorism have a lasting negative impact on EU citizens and come at a high social cost.

What are the links between terrorism and extremism and serious and organized crime?

They are characterized by the sharing of criminal services, a common recruitment pool, an overlap of suspected extremists and terrorists or vice versa and a history of criminals with extremism or terrorism. Terrorists and violent extremists are also involved in serious and organized crime to increase profits and finance terrorist operations^{8 9}.

To understand the importance of Vulnerability Assessment in relation to places of worship, it is crucial to analyse terrorist activities and relevant risk factors on an individual and environmental level.

If you are interested in attack statistics, you will find some valuable information below. According to GTI 2022¹⁰, there have been several distinct phases of terrorist activity over the past two decades.

⁴ Europol (2016). *Changes in Modus Operandi of IS revisited*. Retrieved on February 2nd, 2016. URL: <https://www.europol.europa.eu/newsroom/news/islamic-state-changing-terror-tactics-to-maintain-threat-in-europe>

⁵ European Commission (2020). *Protection of Public Spaces Newsletter: "Terrorism Risk Assessment of Public Spaces for Practitioners"*. Retrieved on April 22nd, 2020. URL: https://ec.europa.eu/newsroom/pps/item-detail.cfm?item_id=674909

⁶ OCHA (2022). *Global Terrorism Index*. p.32-35. Retrieved on July 20th, 2022. URL: <https://reliefweb.int/report/world/global-terrorism-index-2022>.

⁷ OCHA (2022). *Global Terrorism Index*. p.33. Retrieved on July 20th, 2022. URL: <https://reliefweb.int/report/world/global-terrorism-index-2022>.

⁸ European Commission (2017). *Terrorism Situation and Trend report (TE-SAT)*. Retrieved on July 20th, 2022. URL: <https://www.europol.europa.eu/tesat/2017/index.html>.

⁹ Europol (2022). *Terrorism Situation and Trend report (TE-SAT)*. p.19. Retrieved on July 20th, 2022. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf.

¹⁰ OCHA (2022). *Global Terrorism Index*. Retrieved on July 20th, 2022. URL: <https://reliefweb.int/report/world/global-terrorism-index-2022>

Europe recorded:

- Greece was the second most affected country in Europe, with the country recording 50 attacks, an increase of 22 per cent (p.39),
- Germany recorded the second highest number of terror attacks for the region in 2021, and has the fourth highest overall impact of terrorism in Europe (p.39),
- There were 12 religiously-motivated attacks in Europe in 2020 and another 3 in 2021 (p.39),
- In addition, between 2002 and 2010, UK and France were the second and third most affected countries in Europe,
- the main type of attacks by region indicate that bombings and armed assaults are the most common forms of terrorism in most regions.

Picture 2 – Police on duty

According to Europol's TE-SAT Report (2022)¹¹:

- TE-SAT reports from 2021 and 2022, despite the downward trend in attacks on places of worship, still indicate that the biggest threat is still the so-called Lone Actor.
- All of the completed attacks in 2020 were committed by individuals acting alone (lone actors), using firearms or mostly unsophisticated attack methods (stabbing, vehicle ramming, and arson).

Analyses by Europol and the *EU Intelligence Analysis Centre (INTCEN)* confirm that more and more attacks in the EU are carried out in public spaces using everyday objects, such as truck ramming or the use of knives to injure victims. The targets of attacks are "soft targets" selected to cause the largest possible casualties among the civilian population¹².

That is why, for decades, the institutions of the European Union, supported by the activities of governmental institutions of individual Member States, have been taking measures to keep terrorist threats, as much as humanly possible, to a minimum. They are not alone in this struggle. The European Union coordinates and shares its expertise with international organisations such as the United Nations to protect public places, including places of worship.

For more information see:

- The EU Security Strategy¹³
- The Counter-Terrorism Agenda for the EU: Anticipate, Prevention, Protect, Respond¹⁴

¹¹ Europol (2021). *Terrorism Situation and Trend report (TE-SAT)*. p.19. Retrieved on July 20th, 2022. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf

¹³ EU Commission (2020). *EU Security Union Strategy*. Retrieved on August 19th, 2022. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from=EN>.

¹⁴ EU Commission (2020). *A Counter Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond*. Retrieved on August 19th, 2022. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0795&from=EN>.

Figure 2 – Map of terrorist attacks in Europe in 2020

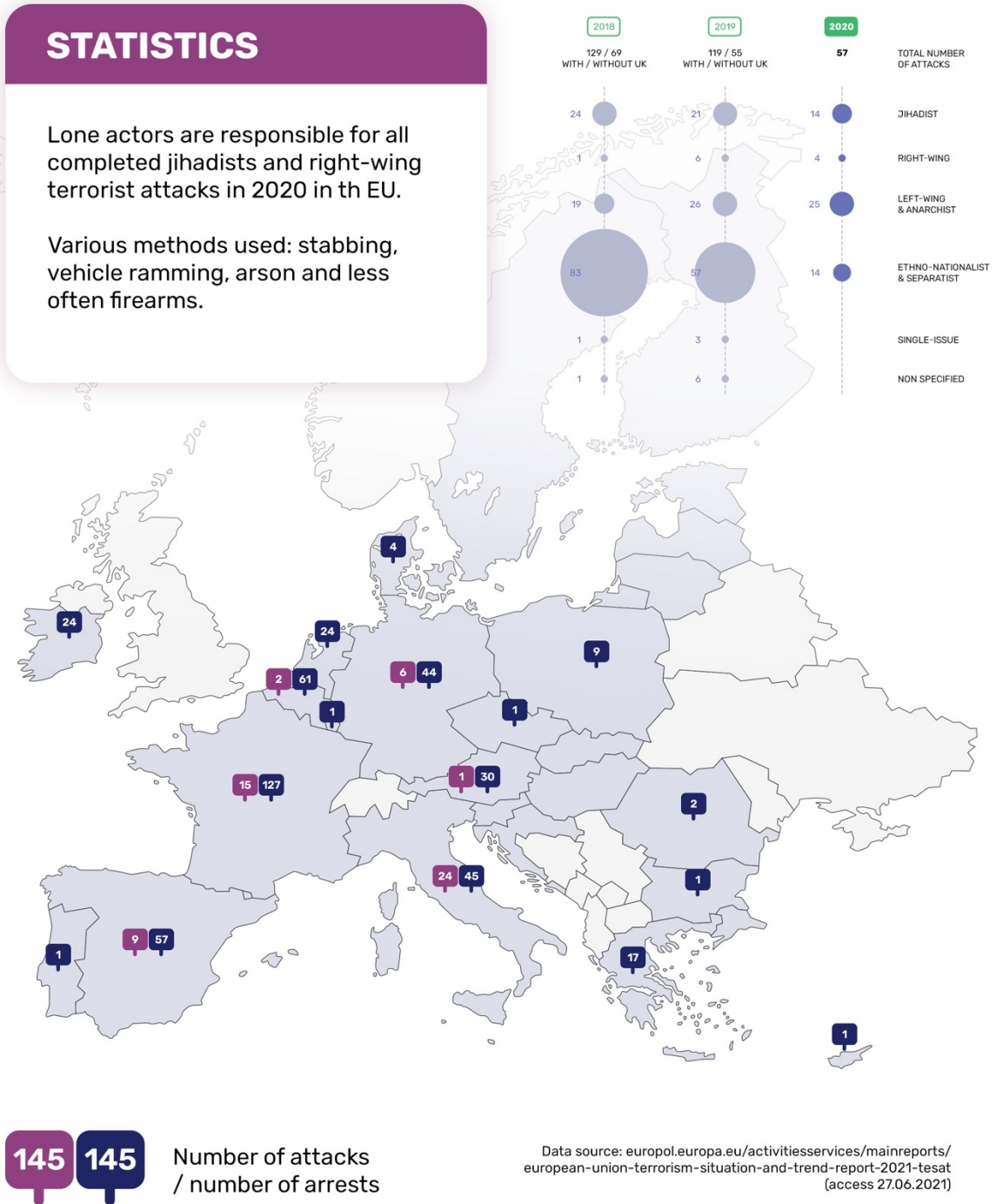
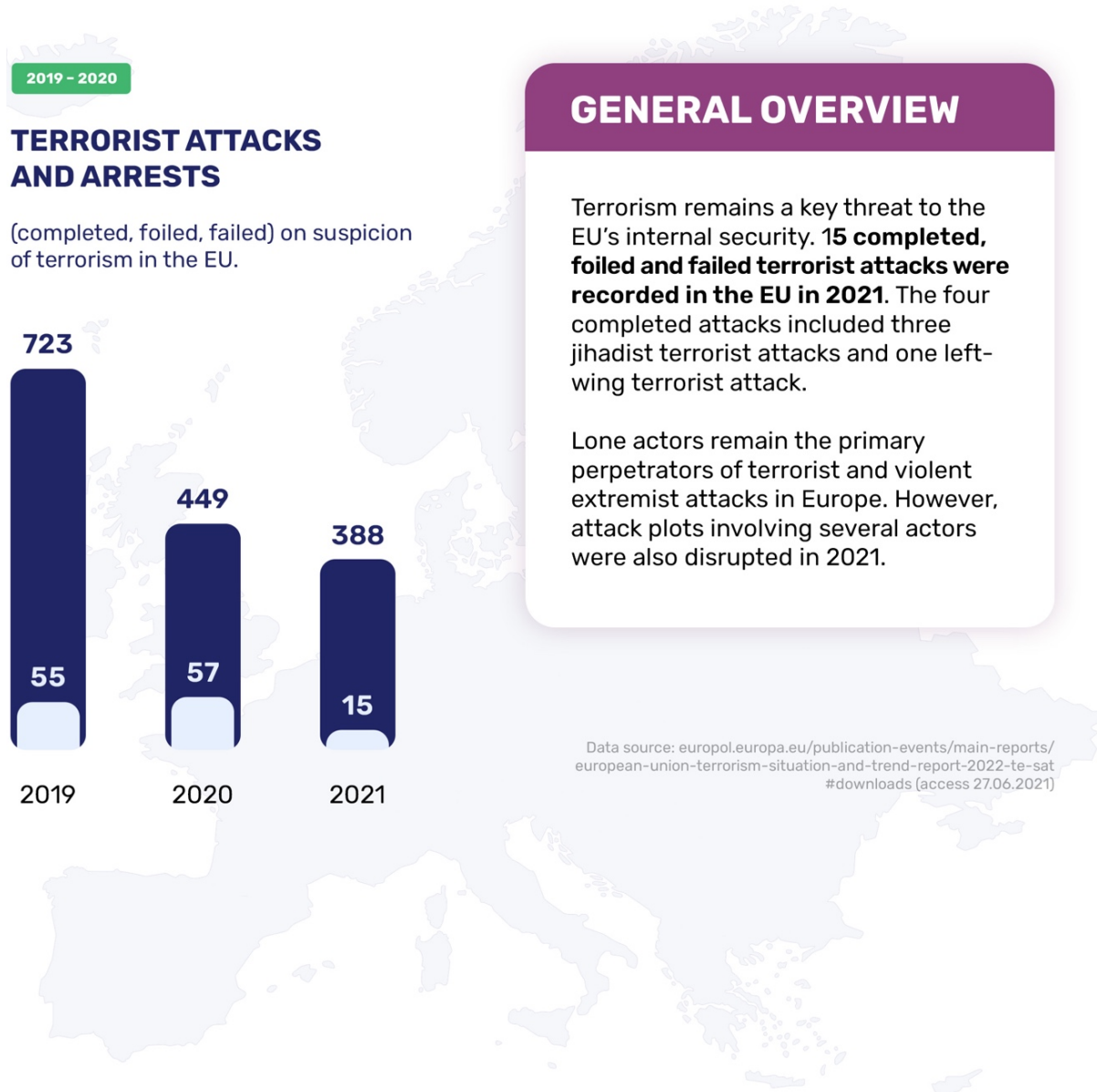


Figure 3 – Number of terrorist attacks in Europe 2019 - 2021



2.2. General information about the ProSPeReS project

By reading this section, you will get an overall outline of the most important facts about the ProSPeReS project.

The project concept addresses the issue of places of worship considered vulnerable to terrorist attacks because of their symbolic value, accessibility and the fact that limited security measures are usually in place. Consequently, they have been the target of extremists in recent years.

Data collected from religious institutions and authorities show a need to strengthen the security of places of worship.

In light of the above, stakeholders involved in the management, protection, safety, and security of places of worship should implement appropriate practices to be aware of these locations' vulnerabilities to potential attacks. This would improve their ability to identify and adopt prevention and mitigation measures against attacks of a terrorist nature, and to implement appropriate practices based on the assessed likelihood and consequences of such threats.

The scope encompassed by ProSPeReS and its activities is in line with the EU Action Plan¹⁵ to support the protection of public spaces, together with the EC Staff Working Document entitled "Good Practices, which also supports the protection of public areas," applied in the specific context of places of worship. Good practices relevant to this type of public space, identified by the EC, constitute the core basis for the project's approach and planned work.

The overall aim is to increase the security of religious sites in the European Union against terrorist attacks. The comprehensive protection system developed within the project works on the assumption that increasing the level of security of religious sites is achieved whilst maintaining the accessibility and openness of these places so believers can worship there.

The system covers measures designed to increase prevention, protection and provide deterrents in order to respond to various terrorist threats and incidents that may occur in religious places, including attacks with CBRN agents¹⁶. For example, the EU VAT methodology was adopted to cater for the needs of places of worship and constitutes a tool for informing executive authorities about tailored and appropriate protective actions based on collectively identified security needs.

The project's aim to increase the level of protection in places of worship has been achieved by forming an outstanding cooperation with scientists, security experts and practitioners, public services, and religious institutions who represent the Catholic Church, Greek Orthodox Church and Jewish Communities to prepare a comprehensive and practical protection system. Furthermore, faith-based partners from the Consortium and other institutions that represent various Muslim, Christian and Jewish communities will be consulted so their input and recommendations can be taken into consideration.

The project includes:

- vulnerability assessments,
- developing a security awareness programme for site personnel, the faithful and competent public security officials,
- the application of the Security by Design concept,
- creating links and synergies with other relevant European Union projects,

¹⁵ EU Commission (2020). *Action Plan to support the protection of public spaces*. Retrieved on February 2nd, 2023. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0612&from=EN>

¹⁶ ProSPeReS GA, p. 94

- preparation and implementation of security, prevention, detection, and response plans,
- recommendations for improvements in detection and protection equipment,
- exercises to collaborate with public services and validate proposed improvements.

The implementation of the system will be improved by preparing and initiating the following:

- distributing guidebooks and recommendations to the public (mainly to the PW communities),
- preparation of modular training, including e-learning with VR, applicable in various types of education in religious structures,
- conducting large-scale exercises,
- running a pan-European awareness-raising campaign targeting religious leaders, believers and the general public.

Recommendations issued by other international organisations (e.g., the International Conference "Safety and Protection of Religious Assemblies and places of worship", which has been organized by the consortium partners annually since 2015; Action Plan for the Protection of Religious Places, 2019) was the subject under consideration and also the inspiration for the Guidebook. They call for the development of appropriate products and tools, such as general guidelines for specific measures to protect places of worship, the development of joint training sessions, communication networks, information sharing, and early warning mechanisms and building partnerships with religious leaders and government officials to raise awareness of how to prepare for and respond to attacks on places of worship. All aspects are thoroughly operationalized in the relevant practical arrangements foreseen in the project.

The consortium consists of institutions with different, significant profiles, representing different faiths from six European Union countries from all over Europe (north: Finland, south: Greece, Cyprus, west: the Netherlands, central east: Poland, Slovakia). The strength of the consortium is the contribution of different cultures, traditions, religious practices, and its diverse approach to religion. More at: www.prosperes.eu

Moreover, the project is strongly supported by already existing, influential networks of institutions from other countries, as well as at the international level. The religious institutions of the Catholic Church represented by the Archdiocese of Łódź, the Jewish Community of Warsaw and the Holy Metropolis of Ioannina (the Greek Orthodox Church) that are part of the consortium play a key role and make a key contribution to the project. In addition, the project has received important support from Vatican officials (such as the Undersecretary of State), COMECE (EU Bishops' Conference Commission), and the Cypriot Orthodox Church. Other religious organisations have also participated in selected project activities:

- Catholic Church from Wrocław and Białystok.
- Lutheran Church from Poland.
- Evangelical Church of Finland.
- 'Faith Matters' organisation from the UK.
- The Church of Greece Representatives of the Jewish community from Leiden and Copenhagen, and the European Jewish Congress.
- Leaders of Dutch Muslim communities.

The project's approach is to prepare an appropriate, well-targeted, and validated protection standard and ensure its EU-wide benefits for the protection of religious sites through cooperation between key stakeholders. Therefore, the consortium consists of a large number of organisations, currently totalling 18, representing scientific and expert institutions, public services such as the police, fire brigades, and crisis management, as well as end users - religious institutions and operators of places of worship.

The project programme consists of 8 work packages (WP). WP1 covered project coordination, administration and quality assurance, while the remaining five WPs were strictly focused on achieving the project objectives. In WP2, the consortium identified the current state of and protection needs by assessing vulnerabilities, gathering information, conducting surveys, and sharing best practices. Then, in WP3, system elements were prepared, such as a Security by Design guide, a set of procedures, hardware recommendations, and cooperation protocols, which were consulted and approved by religious institutes. WP4 focuses on preparedness for CBRN protection. The WP4 aims to increase the awareness of religious sites' staff of CBRN agents. Moreover, the prepared reaction model will be a guide for the response in an actual CBRN crisis situation.

A training programme with face-to-face and e-learning materials was created and piloted in WP5 to initiate cascade training. Evidence-Based System Validation (WP6) was conducted as a large-scale exercise in collaboration with religious sites and public services. It included high-level and real-world activities during the evaluation sessions, including clearance. Awareness raising is an integral part of the project, Therefore a separate WP7 is planned for the entire project duration. The awareness campaign included the preparation of a strategy, a set of brochures and web materials, the use of social media, and the organisation of workshops, seminars, and presentations to raise risk awareness and develop key protection measures. Finally, the last work package (WP8) is devoted to ensuring the sustainability of the project by taking into account its dissemination (related to WP7 activities), intellectual property rights, and compliance with personal data protection and ethical principles.

2.2.1 WP3 objectives

The WP3 – Preparing tailor-made security measures for religious sites consists of the following:

- A.3.1 Analysis and assessment of the relevance of the state-of-the-art achievements in public places protection – Security by Design, novel detection technology, equipment, PPE, procedures and training, and cooperation protocols.
- A.3.2 Preparing the Security by Design guidebook for religious sites.
- A.3.3 Preparing the set of procedures to prevent, protect, detect, respond to and mitigate the results of terrorist attacks.
- A.3.4 Preparing recommendations for equipment – monitoring, detection, and protection.
- A.3.5 Preparing protocols for communication and cooperation with public services.
- A.3.6 Conducting workshops with stakeholders to validate the results.
- A.3.7 Introducing changes according to received feedback.

2.3. Results of ProSPeReS workshops and case studies regarding various places of worship

The ProSPeReS Work Package 2 (WP2) – The Vulnerability Assessment & Needs Analysis of Religious sites. The conclusions from the implementation of WP2 provided the knowledge basis for WP3 and WP6. WP2 was essential for the design and development of WP3. The main goal of WP3 was to prepare a comprehensive set of security measures using WP2 findings and relevant EU activities regarding the protection of Places of Worship¹⁷ (surveys, workshops and case studies).

Survey

The observations and knowledge collected during the workshop and case studies were highly important for determining the current state of security in places of worship, identifying gaps and needs, and implementing vulnerability assessments (VA) and risk analyses.

The VAs were carried out based on the methodology of the Vulnerability Assessment Tool¹⁸ / Checklist (VAT)¹⁹ developed by DG HOME and made available to ProSPeReS for research purposes. The objectives of WP2 are the exchange of good practice examples in current security systems and the identification of a common set of needs and gaps evident at various places of worship²⁰ that need to be addressed to enhance the offered level of security across the EU. Specifically, the aim of the VAs was to identify security weaknesses at selected religious sites and propose measures to eliminate them and prevent a potential crisis in case of an attack carried out by various means. The sites used as case studies for the workshops were indicated by the religious consortium partners of ProSPeReS and validated by the rest of the consortium. The choice of the sites was made based on their significance for the local communities and upcoming high-profile events which are scheduled to take place, and which will lead to large gatherings. The participants of VAs consisted of representatives from various local LEAs, first responders, and municipal authorities responsible for or involved in the protection of the selected sites, including the sites' operators and religious staff.

Additionally, study visits to selected places of worship were conducted to collect additional information about Security by Design issues by using questionnaires. By means of a survey, it was possible to obtain answers to the following questions:

- What elements of Security by Design are most common in the PW?
- What are the most common good practices in the PW?
- What are the most common gaps in the PW?

In addition, as a result of the questionnaire survey, it was possible to identify restrictions in the context of using Security by Design solutions. The study visits also proved that while addressing the protection solution, the different backgrounds of religious communities as well as the different types of buildings and locations should be considered.

¹⁷ European Commission (2021). EU Quick Guide to support the protection of Places of Worship. Retrieved on July 22nd 2022. URL: https://home-affairs.ec.europa.eu/document/download/8a4ef2e6-12ff-446d-9df5-1ce164adab25_en?filename=EU%20Quick%20Guide%20to%20support%20protection%20of%20Places%20of%20Worship_en.pdf

¹⁸ Not publicly available at the time of this manual's conduction.

¹⁹ In 2021 the VAT was updated and renamed Vulnerability Assessment Checklist (VAC). The updated version was made available well after the beginning of the project. However, VAT and VAC follow the exact same methodology with the addition of extra information for consideration found in the updated version of the tool.

²⁰ The terms religious sites and places of worship are used interchangeably within the report.

Identified faith-based objects include:

- Single freestanding buildings, such as a typical mosque;
- A complex of free-standing buildings, typical of Roman Catholic parishes;
- A PW constituting a sanctuary;
- A PW that is also an educational centre;
- A PW in a multi-store building.

Important findings:

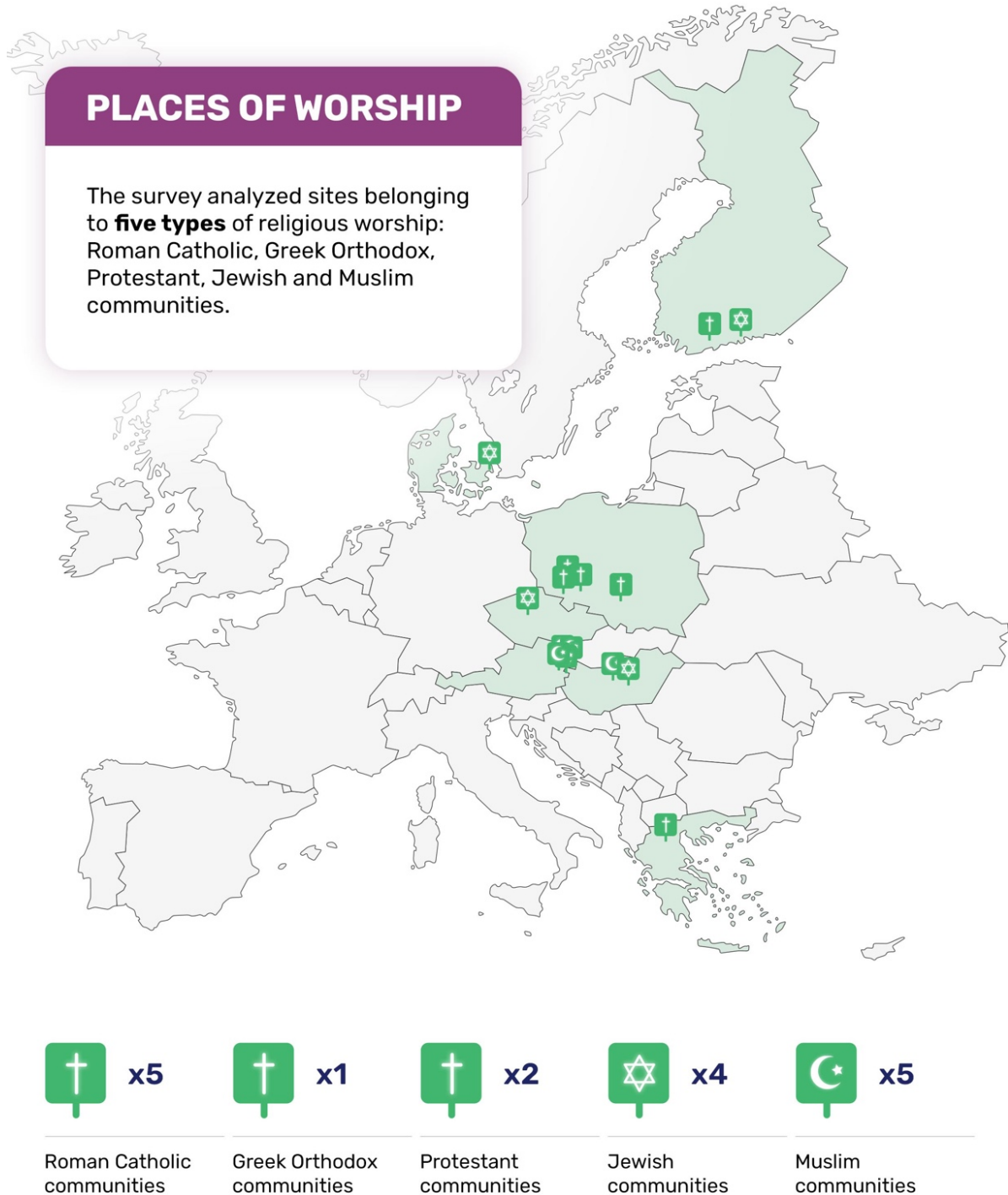
The survey made it possible to identify the most common potential security gaps in a place of worship, as well as to identify good practices whose implementation in other places of worship may reduce their vulnerability to terrorist attacks.

Conclusions drawn from the analysis of findings facilitated implementation of protection measure recommendations that are as universal as possible and can be easily applied to any PW, regardless of religion, form of religious worship, size, architectural style, or building type.

Picture 3 – Large gathering



Figure 4 – Map of surveyed places of worship



The most common security and security vulnerabilities identified by the survey:

- Insufficient number of emergency exits or emergency exits designed only to meet fire regulations (they do not fulfil their functions in the event of a terrorist attack);
- Existence of side entrances that are not adequately secured and may allow unnoticed or unauthorized entry to the building;
- Possibility to leave the facility unattended inside the building;
- Possibility to leave the facility unattended near the building and people can hide near the building;
- Lack of any form of window protection;
- Easy access to installations, e.g. gas installations;
- No plan of the facility visible;
- Limited supervision of the parking lot;
- Lack of access control to public car parks;
- In one case, an unprotected gas pipe was observed outside the building facade which was vulnerable to unrestricted interference.

Workshops and case studies

Participants of the workshops consisted of ProSPeReS consortium representatives and local stakeholders involved in the protection of the religious sites. During the workshops and case studies, the participants had the opportunity to familiarize themselves with and actively engage in the process of conducting a Vulnerability Assessment (VA) in selected places of worship.

The VAT was based on the EU Vulnerability Assessment Tool²¹ (EU VA Check-list) developed and made available by DG HOME, which aims to enhance the protection of religious sites (places of worship including their surroundings) from terrorist attacks.

The workshops and case studies were a valuable opportunity for participants to see a wide spectrum of risks and threats being analysed in accordance with VAT.

The workshops and case studies' main objective, as in previous activities, was to identify the selected PW's vulnerabilities against potential terrorist attacks and to allow the site operator and the competent local stakeholders to consider appropriate solutions for the site's protection. During the workshops all eight threats/attack types included in the VAT were individually assessed for each identified zone in or around the place of worship:

²¹ Not publicly available at the time of this manual's conduction.

Figure 5 – Threat types**FIREARMS
ATTACK**

(e.g. small calibre pistol
or semi/fully-automatic
rifle- AK47)

**SHARP OBJECT
ATTACK**

(e.g. knives, machetes,
other sharp or blunt
objects)

**VEHICLE
ATTACK**

(e.g. use of the vehicle
as a weapon by ramming
large crowds)

**IED-
EXPLOSIVES**

(e.g. placed / concealed
in objects or goods)

**PBIED-
EXPLOSIVES**

(e.g. explosives
concealed on a person
(suicide or carrier)

**UAVIED-
EXPLOSIVES**

(e.g. remotely controlled
device - explosives or CBR
threats carried and spread)

**VBIED-
EXPLOSIVES**

(e.g. explosives
concealed inside
a vehicle (or its cargo)

**CBRN**

(e.g. threat object concealed
in goods or carried items - e.g.
teargas canister (chemical),
concealed in goods or carried
items (biological), threat object
concealed in goods or carried
items (radiological, threat).

3. Multi-stakeholder and community cooperation

Picture 4 – Diverse religious community



3.1. Introduction to the cooperation

It is worth knowing how to support the surrounding environment and communities for the common good, which is to increase the level of security of, among others, places of religious worship. It may often turn out that people from outside our immediate community are also the beneficiaries of our activities. Thanks to this, we can count on their support and interest in our projects. By skilfully engaging all potentially interested parties to act, we will obtain a coherent, uniform system that will improve the security of sacred places important to our community.

In chapter 3, we will:

- suggest to YOU some useful definitions and give YOU some useful theories – 3.2.
- suggest to YOU why establishing good communication between multi-stakeholder and good community cooperation is important to increase the security of religious sites – 3.3.
- suggest a way for YOU to build and manage multi-stakeholder and community cooperation – 3.4.
- resume all of the above – 3.5.

3.2. Definitions and theory

Safety and security

According to Abraham Maslow²² “One of the basic human needs is a sense of security” - each subject must experience a sense of security in order to be able to meet other needs. According to his theory, security is aimed at ensuring the existence and the implementation of tasks set by a given entity.

Security is undoubtedly one of the most highly valued objectives for both individuals and nations. There are many and at times competing definitions of the term. On the one hand, security often refers to the protection of individuals, organisations, and assets against external threats and criminal activities. It is the protection from directional, deliberate threats by conscious agents aimed to inflict harm on an individual, organisation, or its assets. Safety, on the other hand, means the protection from operational hazards and harmful environmental influences. Some scholars, however, argue that safety should be considered as the absence of harm and risk and security merely as the means to achieve safety. In that sense, safety obtains a more comprehensive meaning (for a discussion see Marcuse 2006²³).

It is this lack of definitional clarity that has been cause for critiques for decades (see e.g. Wolfers 1952²⁴). In the wake of 9/11 terror attacks and the perceived blurring of domestic and international security spheres, governance and sovereignty issues have gained increasing attention. The question to what extent security can still be the prerogative and responsibility of the state vis-à-vis civil society or even individual citizens has been at the core of urban security arrangements since, with a tendency to shift more responsibility to the latter in an attempt to build local resilience against threats that seem undefined in space or time (see Graham²⁵ 2010; Coaffee 2016²⁶; Kienscherf 2017²⁷).

Who are stakeholders?

Several theoretical definitions can be cited here. Therefore, for the purposes of this guidebook stakeholders are all those people and organisations that can affect, be affected by, or perceive themselves to be affected by the activity and functioning of a given place of religious worship; both in private and administrative matters.

Stakeholders refer to anyone who represents a group or association with shared interests.

Stakeholders are persons or organisations that can affect, be affected by, or perceive themselves to be affected by a decision or activity²⁸.

Thus, a stakeholder is every:

- clergyman / clergyperson, imam, rabbi;
- employees or worshippers;
- individual members of a religious community;

²² Maslow, A. H. (1943). A theory of human motivation. *Psychological Review*, 50, 370–396.

²³ Marcuse, P. (2006). Security or Safety in Cities? The Threat of Terrorism after 9/11. *International Journal of Urban and Regional Research*, 30(4), 919–929. <https://doi.org/10.1111/j.1468-2427.2006.00700.x>

²⁴ Wolfers, J. (1952). “National Security” as an Ambiguous Symbol. *Political Science Quarterly*, 67(4), 481. <https://doi.org/10.2307/2145138>

²⁵ Graham, S. (2010). *Cities Under Siege: The New Military Urbanism* (1st ed.). Verso.

²⁶ Coaffee, J. (2016). *Terrorism, Risk and the Global City: Towards Urban Resilience* (1st ed.). Routledge.

²⁷ Kienscherf, M. (2017). *US Domestic and International Regimes of Security: Pacifying the Globe, Securing the Homeland*. Taylor & Francis.

²⁸ International Organisation for Standardization (2009). ISO 31000:2009 – Risk management – Principles and guidelines. Retrieved on February 2nd, 2022. URL: <https://www.iso.org/obp/ui/es/#iso:std:iso:31000:ed-1:v1:en>.

- neighbouring communities and housing communities surrounding a place of worship;
- Law Enforcement Agencies/Authorities – LEAs (Police, Gendarmerie etc.) & Fire Service;
- units of central administration.

Stakeholders are a cooperative and close-knit group who play a significant role in maintaining the level of security of a place dedicated to a given religious denomination. This is because strong and well organised local or religious communities are not only an essential element of a democratic society but most of all, a partner that effectively supports the activities of uniformed services and central authorities aimed at counteracting and combatting terrorism or crime. And it is one of the most important factors affecting the safety of individuals, communities, and specific places, including places of worship.

Achieving good cooperation requires identifying individual stakeholders and identifying the best possible practices for their cooperation.

Usually, a place of worship is looked after by a clergyman or a group of such people.

A priest, rabbi, imam, or other clergyman managing a given place of religious worship is one of the most important links whose initiative and organisational skills determine the success of building cooperation not only in a group of believers but also with the local community, which depends on whether this person:

- knows their subordinates who lead prayers and religious ceremonies;
- knows the faithful participating in the religious life of the place of worship;
- knows the neighbourhood adjacent to the place of religious worship;
- knows most of the people in the neighbourhood and can assess who are well disposed towards a place of worship in their local community, who are neutral and who downright hostile to it;
- who is in contact with other organisations, NGOs, local authorities, LEAs, central authorities, representatives of various types of emergency services, law enforcement or other domestic or foreign institutions.

Very important stakeholders are neighbouring communities and housing communities surrounding places of worship. The inhabitants who create them do not necessarily have to be associated with the religion of the places of worship. However, despite their different beliefs, sometimes they have a common interest in these places, namely, the safety of their home, family, and estate. Obtaining their support and commitment is possible if we clearly define a common goal, which is to ensure everyone's safety and that of the community in which the places of worship are located.

Knowledge of outsiders should never be ignored or underestimated. They may be neighbours who do not follow our religion, but this does not mean that as people they do not care about the safety of their neighbourhood. Building relationships with all players based on common interests (safety of the neighbourhood, district) can lead to a collective and more effective effort toward the protection of an area.

Depending on the status of a place of religious worship additional stakeholders might be:

- private companies providing supplies, assistance or performing various types of services, e.g. security, maintenance, management, etc.;
- NGOs cooperating, in particular, in various types of aid programmes, e.g. counteracting drug addiction, prostitution, crime, support for the homeless or starving, etc.;
- local authorities or local officials;
- central administration and their representatives;
- emergency services (Emergency Medical Service, technical support etc.);
- others.

Community safety and community policing

Community policing has proven²⁹ to be a very effective measure when you are trying get a good information position (who might be showing behaviour that can indicate radicalization) and to fight the crime paradox³⁰ in society. The crime paradox describes how elderly females for instance, are most afraid to become targets of crime, while young males show up most frequent in crime victimization statistics. With community policing, Police can show citizens not to worry and at the same time can protect those that do not worry, but need protection.

Note:

Community safety is much more than just community policing and enforcement.

Community safety requires that each citizen plays a key role in both their own safety and the safety of others.

Community participation and a high level of coordination between government and non-government community resources to identify and respond to the needs of the community are essential ingredients for overall success. Success requires the mobilization of local stakeholders.

The local community is often interpreted as forms covering the entire life of the inhabitants, shaping the systems of responsibility of groups and institutions, and enabling its members to meet their needs. It is about taking advantage of favourable circumstances and taking up challenges, as well as reducing the likelihood of failure by preventing and countering all kinds of threats that may affect the entity's achievement of its goals.

Local stakeholders are involved with community cooperation at a grassroots level.

²⁹ Politie Academie (2016). Best of Three worlds. Retrieved on February 2nd, 2023. URL: <https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/92891.PDF>

³⁰ Kappes, Cathleen. (2012). *Disentangling the Victimization-Fear Paradox : An Emotional Developmental Perspective on Precautious Behavior*.

The philosophy of community policing is understood as a closer relationship with citizens through the constant presence of police officers close to the citizen, and the local community. Poland provides an example of community policing and has created a National Map of Security Threats as part of its activities. This is a typical IT tool that serves as a communication system between local communities and the Police, which allows users together with the Police to properly identify and present the scale and type of threats they face. Cooperation with external entities has a significant impact on the implementation of the statutory tasks of the Police in the field of ensuring the security and public order of the state. The National Threat Map facilitates the creation of the educational role of the Police and the involvement of citizens in shaping public safety and order. It ensures a neutral, often anonymous dialogue between the police and the public that builds mutual trust and increases awareness of the real impact of building security in a democratic society with the participation of all entities involved in this process.

In this respect, the influence of stakeholders and the role they play in the processes of smart and safe city development are important. The local communities, economic entities, scientific institutions and municipal enterprises are important for the safety of the city at every stage of its operation.

Picture 5 – Security staff on duty



3.3. Tips for good communication

Why is it important to establish good communication and cooperation between multiple stakeholders and the local community in order to increase the security of places of worship? The painful experiences of terrorist attacks and other crimes and acts of violence directed against places of religious worship have made people realize the enormous role of individual and local organisations, unions, associations, NGOs in preventing and eliminating the effects of such acts. This is especially true in democratic societies. The authors of the handbook, based on their professional experience, subjectively believe that people are becoming better educated, trained and aware. They are realizing that their quality and living standards, including their personal safety, increasingly depend on their initiative. This also applies to religious communities, even though their main goal is the spiritual development of their members.

Safety and security providers need to take a fresh look at law enforcement methods and the way security services relate to the larger environment in which they operate as one of a variety of institutions fostering public safety and security.

Why are multi-stakeholder and community cooperation so important? Because personal awareness and accountability, rather than looking elsewhere for solutions, have emerged as key ingredients of a successful strategy.

The most effective personal tactics to enhance safety are often the simplest. Communities have frequently identified manifestations of this such as the way people feel connected to others by participating in the community, knowing their surroundings, and promoting an individual sense of citizenship. There is an acceptance that every single person regardless of their function or profession who participates or does not participate in the activities of a given community affects the safety of the general public, which is crucial for increasing the level of safety of the entire community.

It is very important to understand that ensuring security starts at the lowest level. Security services cannot be everywhere. In democratic countries, it is the commitment of the individual, the joining of individuals into groups or communities focused on the implementation of a common goal that constitutes an irreplaceable contribution to building the security of the area. Such communities, having knowledge and knowing how to support it, create a tight, pragmatic, and professional security system.

This also involves a proactive stance on the part of the citizens in which they do not wait for security services to approach and solve their problems. Instead, they use their agency to provide for their own security as much as possible.

Such practices rest on the realization that law enforcement and security services are neither omniscient, omnipotent, nor omnipresent. In other words, they cannot be everywhere and know or do everything. Even in totalitarian countries, security services have numerous limitations. Democracy gives many privileges to individuals but also requires commitment from them. Each and every individual has a far-reaching capacity to choose to act or not.

However, for multiple stakeholders to be effective together, they need to know how to communicate and collaborate to ensure and maintain a level of safety appropriate for their community.

The practice of many EU Member States, which already implement neighbourhood crime prevention programmes, proves that the cooperation of local communities with the police and creating an appropriate climate by building mutual trust effectively prevent and combat crime.³¹ Strong and well-organized local communities are an important element of a democratic society. Therefore, in ensuring the safety and public order of places of religious worship, the cooperation of the faithful gathered in a

³¹ Davey, C., Wootton, A.B., Guillén, F. Diniz, M. and van Soomeren, P. (2019) D2.4. Review of State of the Art: Community Policing, Cutting Crime Impact, Retrieved from https://www.cuttingcrimeimpact.eu/download/24-june-2019_d24_1014042550.pdf.

given community and the establishment of rules of cooperation with the local community living near the place of religious worship is very important.

3.4. Suggestions on how to build and manage multi-stakeholder and community cooperation

If you want to involve stakeholders in cooperation or establish permanent cooperation within the local community, it is best to start by:

I. Defining your vision and goal

For this guidebook, we assume that your vision is to have a safe place of worship.

The goal is to:

- increase awareness and knowledge about safety;
- establish multilateral channels of communication and information exchange between stakeholders and communities;
- create local cooperation, involving all stakeholders.

II. Choosing a leader

Firstly, it is necessary to provide a serviceable definition of a leader. Each implementation of a plan or strategy requires a clearly defined leader - a project manager. Of course, this person should not be selected at random, but be someone with proven competencies in implementing other projects or strategy implementation. The leader most often becomes a person:

- managing a place of religious worship;
- entrusted with the preparation of ceremonies;
- who is assigned to manage safety;
- who belongs to a given religious or local community;
- who is a committed person in matters relating to the religious site.

Leaders need to be able to present their initiatives, propose various types of organisational activities and use their commitment and skills to strengthen the security of a given religious place using evidence-based solutions which focus on the security of places of religious worship and believers. The most interesting will be strategies related to counteracting and combating terrorism, extremism and crime.

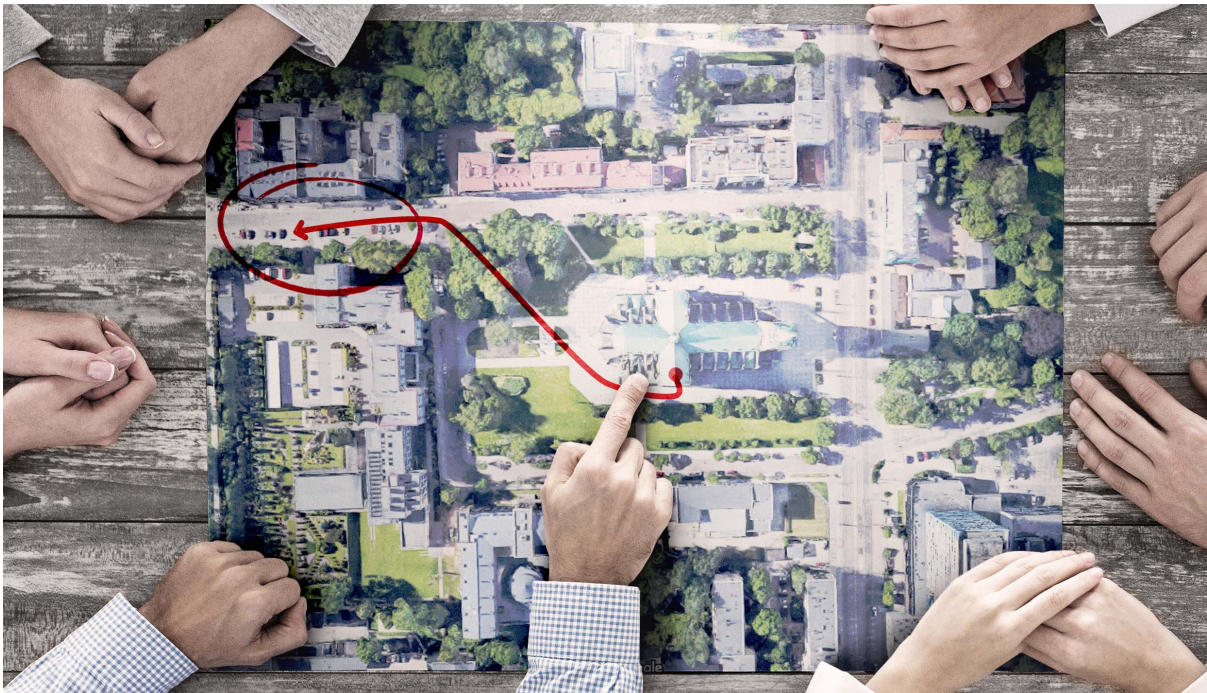
For example, many strategies assume that representatives of central or local authorities (depending on the needs) will have to be involved at some level. This might be, for example, the mayor, city council, or local police chief. However, the active involvement and participation of the local community are of key importance in identifying and responding to local safety problems. In fact, the community is at the heart of successfully preventing attacks or crime.

III. Creating the plan

Before we create a plan, we should gather up-to-date information about the place of worship whose security level we want to increase.

Such an initial assessment or a more extensive audit of the existing infrastructure allows for a reliable assessment and verification of the technical equipment, procedures and additional security measures. Only after having collected the above information, can we proceed with further planning.

Picture 6 – Crisis team figuring out a plan



Most organisations or project managers create plans based on basic answers to the questions: Who? What? How? When?

Example of a plan:

1. What do we want to achieve; what is our goal? Increasing the security of a place of religious worship through multi-stakeholder and community cooperation:
 - Increasing awareness and knowledge about activities so that places of worship can be made safer; for both individual stakeholders and our entire religious community.
 - Increasing awareness and knowledge of activities so that places of worship can be made safer for people who do not belong to our religious community or are not followers of our religion, but who live in the neighbourhood where our places of worship are located.
 - Establishing channels of communication and information exchange with local and central authorities (law enforcement, emergency services).

2. Who will be a leader?
3. What competencies are we looking for in the community?
4. How will we implement our plan?
 - How many people are needed to implement the strategy?
 - Officials?
 - Volunteers?
 - Professional organisations with whom we will establish contact and obtain support?
5. Who are the most important recipients?
 - Individuals from among our faithful and people living in the vicinity of our places of worship.
 - Local communities such as housing associations, organisations and associations based and operating in our neighbourhood.
 - Local governments and local authorities where our places of worship are located.
 - Police and emergency services stations whose operating zone covers the location of our places of worship and the central authorities or law enforcement agents responsible for ensuring the security of the places of worship in a strategic sense and who are therefore territorially responsible for security.
 - Who else outside the local community is needed to achieve our goal?
6. How do we want to achieve this?
 - What milestones do we aim for on the way to our strategic goal?
 - Establishing contact with the above recipients, e.g. organizing meetings, visits, training.
 - Conducting an information campaign, e.g. via the internet, leaflets, posters (this especially applies to the neighbourhood community).
 - Creating two-way communication channels, defining how and to whom we need to report information about observed events or people that may be important for the safety of our places of worship.
 - Conviction of commitment and cooperation for our cause - it is especially important to convince people from the neighbourhood who do not belong to our community but live near places of worship to be observant and notice things that differ from the typical routine of a housing estate.
7. How will we conduct an information campaign?
8. How will we educate the interested and involved? Education is understood as activities undertaken (e.g. meetings, training courses, information) aimed at increasing the awareness of individuals and a given community; educating them to the required extent, increasing the sense of responsibility for a given community and preparing for practical action.
9. What deadlines will we set ourselves?

It is important to define the deadline for implementing each action.
10. How will we check if our plan is being implemented?

Achieving the assigned tasks within the specified deadlines.

IV. Implementing a plan or strategy

To implement a plan or strategy, it is vital for all audiences that the planner/strategist:

- is clearly understood. That is, succinctly, offer specific and clear language. It should address the root causes of community safety problems.
- is pragmatic in their approach. The strategy should be realistic, based on realistically identified problems and threats. It must be as easy to implement as possible.
- engages individuals and entire communities (neighbours, local authorities, other local organisations, central government, emergency and uniformed services).

The entire community should support the strategy or it will remain a worthless document. The best plan and strategy is the one that works so it is not enough just to develop the best strategy or action plan. Effective implementation is a much more important stage.

The implementation of our plan to increase the security of places of worship with the participation of multiple stakeholders and community cooperation is based on Ronald V. Clarke³², and as usual, strong emphasis is placed on influencing potential criminals or terrorists by:

- making it more difficult (increasing the workload) for the potential perpetrator of the crime to commit a criminal act,
- increasing the degree of risk for the potential perpetrator of the crime,
- limiting the level of benefits from committing a crime,
- reducing the influence of stimulating factors on the potential perpetrator,
- making it difficult for the perpetrator to justify his behaviour.

3.5. Summary 3.2.- 3.4.

Establishing good communication between multiple stakeholders and building community cooperation is vital for strengthening the security of religious sites.

It should be remembered that any programme, not only in terms of security, must:

- be developed, communicated and made available to all involved,
- be accepted by community residents.

Activating the society and involving it in the issue of creating security for local communities assumes that the reference point for our behaviour are reactions to the behaviour of other people.

The more people act in a certain way, the easier it is for others to behave similarly as it is difficult to oppose a trend. Consequently, this makes it easier for individuals to decide how to behave or what to think.

³² Von Hirsch et al. (2000). *Ethical and Social Perspectives on Situational Crime Prevention*. Hart Publishing. Retrieved on December 29th, 2022. URL: http://www.jus.unitn.it/USERS/dinicola/criminologia-ca/topics/materiale/dispensa_1_2_ING.pdf

Nowadays, when developing community cooperation, you can use ready-made patterns. Community policing is especially effective in the European Union. It emphasizes the role of government and local government administration bodies in safety education, the main goal of which should be to increase social awareness and acquire the ability to coexist alongside potential threats that may occur in a given local community.

The freedom to initiate and participate in the design of crime prevention plans and programmes that communities now enjoy is an expression of democracy and civil society.

A local community is created by residents living in a small territory, e.g. a town, or a housing estate, with a similar standard of living and culture. It is a group where there are strong ties as a result of shared interests and needs. These communities have their own goals, tasks and problems to solve. All this means that getting to know members of this community and communicating with them provides enormous possibilities for them to influence their local environment, including its security.

Picture 7 – Checking the security list



For best results, confirm that decisions made in the name of community safety meet the following conditions:

- Evaluate existing relationships and cooperations. Consider which currently functioning elements work and which need improvement. Always take steps after analyzing current solutions, relationships and agreements;
- Establish cooperation and build partnership relations with as many people and communities as possible within the local operational vicinity of our places of worship;
- Designate leader and contact persons and ensure that all interested parties can easily find their contact details;
- Define the goals and missions that need to be achieved;
- Create an action plan according to the above-recommended criteria;
- Implement the plan;
- Raise the knowledge of everyone involved through training, lectures, meetings and information exchange.

Do not forget how important personal involvement in building a security policy is. The state has taken on the indirect role of enabler, promoting the principle of 'self-help' with the private sector filling the vacuum left by the withdrawal of public funding. Increasingly, private sector organisations have become specialists in preventative work, developing solutions to confront and combat crime, which can be sold to the private consumer, public authorities and law enforcement bodies alike.

In most countries nowadays, there is a growing trend towards law enforcement, security services, and in particular the Police, placing greater emphasis on wider society playing an active role to prevent and combat terrorism and crime.

Joint organisation and implementation of programmes, direct actions and preventative measures are having an impact that is maintaining safety and order in public places and protecting property and the environment.

Organizing joint training and exercises is another form of cooperation. An evident aspect of such cooperation is joint exercises, in which other entities responsible for safety, public order, property and health are participants. Therefore, it is accurate to say that the involvement of individuals and community cooperation tends to increase the security of places of worship.

The support of local communities is necessary for the effective operation of law enforcement agencies. It depends largely on honesty and decisions made by policemen, as well as on the nature of direct contact between citizens and police officers. The assistance and cooperation that public services receive from citizens are necessary because social order is not only the concern of the state and state administration but works towards the common good, which benefits a free society.

4. Recommendations

In this chapter, you will find specific procedures and suggestions about how to carry them out. All procedures and suggestions were created based on the findings of the ProSPeReS project.

IMPORTANT: This chapter is a review of the most important recommendations of the solutions made by the project. They are available in full in the Appendices to this Guidebook or on the project website.

All the materials presented are available to users by scanning the QR-code or entering the appropriate link that redirects you to an individual deliverable.



QR-codes and links can be found throughout this chapter. In this way, the Guidebook's authors provide you with full access to the content of the individual deliverables. You are urged to read all information relevant to you, and use the templates and tools to suit your needs and capabilities.

The ProSPeReS security measures are presented in:

D 3.2. Security by Design Guidebook for Religious Sites.

<https://prosperes.eu/resources/>



D 2.1. Manual for vulnerability assessment and VAT Lite.

<https://prosperes.eu/resources/>



Appendix 1 – Set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks.

<https://prosperes.eu/resources/>



Appendix 2 – Recommendations for equipment – monitoring, detection, and protection.

<https://prosperes.eu/resources/>



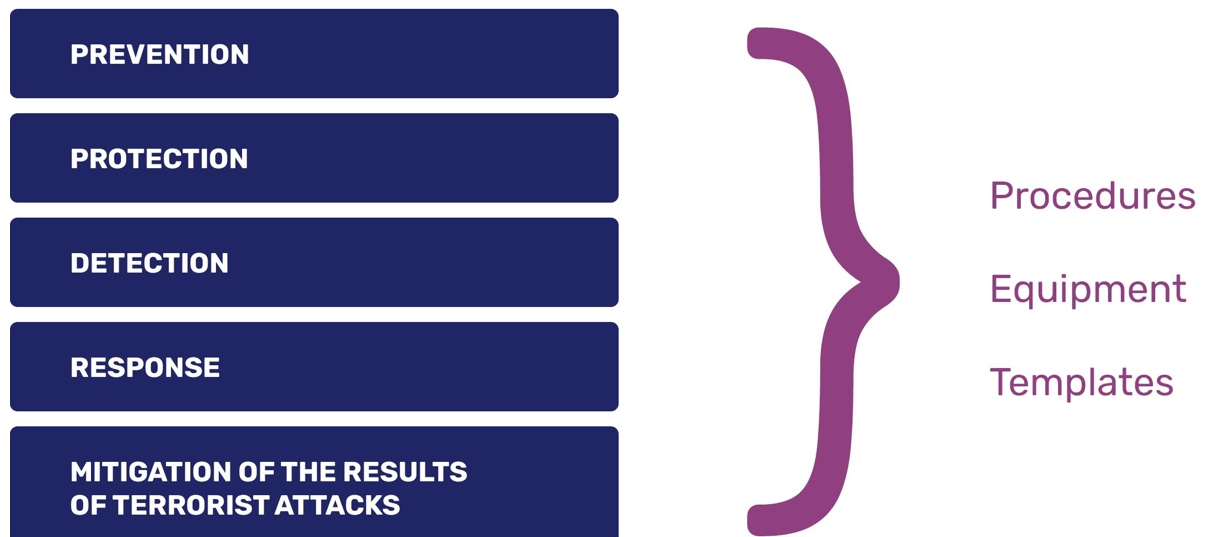
Appendix 3 – Protocols for communication and cooperation with public services.

<https://prosperes.eu/resources/>



Below, you will find the introductory paragraphs about a coherent approach to strengthening the security of worshipers in a PW. You will find all the relevant topics (prevention, protection, detection, respond and mitigation activities) in appendixes attached to the Guidebook – QR-codes and links mentioned above.

Figure 6 – Recommendations



4.1. Prevention

Prevention – in terms of terrorism, EU institutions focus on preventing radicalization, propaganda, financing, public provocation, recruitment, and training. Judging by these factors, we can define prevention as actions by European institutions to stop terrorists from gaining new members by any means and stop members of terrorist organisations from training, taking actions, making provocations, and cutting their financing supply³³.

Referring to the assumptions of the ProSPeReS project, special importance should be given to preventing terrorism (prevention) - understood, in the context of the current considerations, as a set of undertakings of state services, LEAs and local entities, including religious communities aimed at identifying the threat and preventing the occurrence of a terrorist attack through appropriate organisation of the patrol service, social and criminal prevention and multi-stakeholder cooperation with other services, guards, as well as private entities and the local community.³⁴

³³ More at: European Commission, *A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond*, Brussels, 09.12.2020, p. 8.

European Council, *EU measures to prevent radicalization*, <https://www.consilium.europa.eu/en/policies/fight-against-terrorism/preventing-radicalisation/>, [Access: 03.01.2023]

United Nations Office on Drugs and Crime, <https://www.unodc.org/e4j/zh/terrorism/module-5/key-issues/european-region.html>, [Access: 03.01.2023]

³⁴ Based on: R. Batkowski, *Counteracting asymmetric and hybrid threats from the police perspective* [in:] K. Jałoszynski et al. (red.), *Police special forces in Poland*, Szczytno 2015, p.263

“Security by Design”

In this section, you will learn about preventing attacks on places of worship through architectural solutions. Please consider what you can apply or change at your place of worship based on the information below.

Preventing attacks on places of worship should start at the construction stage. However, suppose we manage an already existing place of religious worship, using the information below. In that case, we can decide on ways to modernize the existing structure to obtain the highest level of protection. The best way to prevent attacks on places of worship or limit the effects of an actual attack is to use knowledge from “Security by Design”. It can be used during:

- PW construction planning and design,
- changes during the construction of PW,
- changes made to the infrastructure of the existing PW,
- retrofitting of infrastructure and technical equipment of PW.

Picture 8 – Architectural element: pots and flowerbeds in front of Agios Dimitrios Temple in Thessaloniki ³⁵



³⁵ ProSPeReS project (2022). D 3.2. Security by Design Guidebook for Religious Sites.

Suggestions:

- the best idea is to create a concept that assumes various design solutions to increase the safety of the area around the place (building) of worship.
- it is important to define the main crimes or terrorist threats through the modus operandi of the perpetrators, in the contexts in which the adopted landscaping solutions are considered. The following contextual threats were assumed when making design decisions:

Table 4 – Potential considered threats

Types of attacks	Attack modes
Firearms attack	<i>Attack against a crowd with a concealed automatic firearm.</i>
Sharp object attack	<i>Attack with concealed weapons against a crowd.</i>
Vehicle ramming attack	<i>Attack with a vehicle against a crowd near the main street of a religious site.</i>
IED explosives attack	<i>Attack with a discarded (unattended) bag containing explosives.</i>
PBIED attack	<i>Attack by a suicide bomber against a crowd.</i>
UAVIED attack	<i>Attack with a drone carrying explosive material with the intention of harming a crowd outside a religious site.</i>
Vehicle-Born Improvised Explosive Device	<i>Attack with an explosive material placed inside a car parked near crowded areas.</i>
CBR(N) attack	<i>Attack with chemical agents outside a place of worship.</i>

Please remember:

Traditional facility protection systems focus on their capacity to physically protect a location by separating it into least three concentric protection zones.

If you are interested in more complete, accurate information related to this, go to “D 3.2. Security by Design Guidebook for Religious Sites”, by scanning the QR-code or using the link below.

<https://prosperes.eu/resources/>



For the purposes of this subsection, please pay special attention in D 3.2. Security by Design Guidebook for Religious Sites to the following:

Landscaping elements for the security of a place of worship that can be changed during construction, reconstruction, modernisation or retrofitting:

- benches and other seatings;
- pots and flowerbeds green (grassy or vegetated);
- hills;
- concrete seats interspersed with grass seating and trees;
- stairs with pots, greenery and benches;
- lighting;
- walls;
- fence;
- trees;
- boulders.

Picture 9 – Bollards



If you are interested in more complete, accurate information related to this, go to “Appendix 2 – Recommendations for equipment – monitoring, detection, and protection”, by scanning the QR-code or using the link below.

<https://prosperes.eu/resources/>



Prevention against attacks at organisational, administrative and procedural levels.

In this subsection, users learn how to counteract attacks on places of worship through organisational and procedural solutions. Please consider what you can apply or change at your place of worship based on the information below.

If this is to be prevented, a clear picture is essential to raise awareness of what is needed to help local authorities and other important stakeholders within the sphere of the protection of public spaces to help better protect their public spaces against terrorist threats. This knowledge will help us introduce appropriate regulations and procedures that positively impact our organisation.

Picture 10 – Policewoman helping pilgrims



If you are interested in more complete, accurate information related to this, go to “Appendix 1 – Set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks”, by scanning the QR-code or using the link below.



<https://prosperes.eu/resources/>

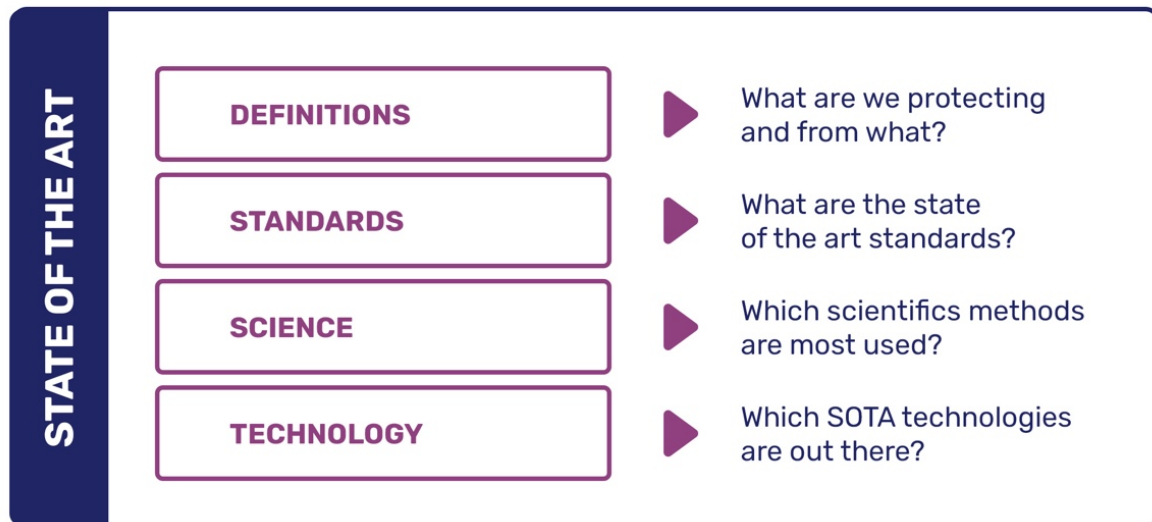
As described in Chapter 3 “Multi-stakeholder and community cooperation,” community cooperation improves the safety of places of worship and is highly important. As a reminder, one of the illustrative schemes is included below:

Figure 7 – Community cooperation³⁶



State-of-the-art analysis gives an overview of the standards, science and technologies used to protect public spaces, which can also be applied to specific types of spaces like places of worship.

³⁶ ProSPeReS Project (2022). *D 2.1 - Manual for vulnerability assessment. Regional stakeholders in the protection of public spaces.*

Figure 8 – State-of-the-art public spaces protection

Identified state-of-the-art standards and protocols are:

- The ISO Risk Management Guidelines 31000:2018³⁷;
- ISO Guidelines for crime prevention through environmental design (CPTED) 22341:2021³⁸;
- The Purple Guide³⁹ – a well-known guide that describes the standards and methods that surround event management,
- The ProSPeReS Deliverable 2.1⁴⁰ “Manual for Vulnerability Assessment”.

If you are interested in more complete, accurate information related to this, go to “D 2.1. Manual for Vulnerability Assessment”, by scanning the QR-code or using the link below.

<https://prosperes.eu/resources/>



The Vulnerability Assessment Tool LITE, created within the ProSPeReS project, aims to introduce a solid methodological approach to conduct the vulnerability assessments foreseen as part of Work Package 2 of the project, for supporting the later identified common needs and requirements to raise the level of protection in places of worship. The approach is based on using the EU Vulnerability

³⁷ International Organisation for Standardization (2018). ISO 31000:2018 – Risk management - Guidelines. p.11. Retrieved on August 11th, 2022. URL: <https://www.iso.org/standard/65694.html>

³⁸ International Organisation for Standardization (2021). ISO 22341: 2021 – Security and resilience – Protective Security – Guidelines for crime prevention through environmental design. Retrieved on August 11th, 2022. URL: <https://www.iso.org/standard/50078.html>

³⁹ Food, Events and Things (2022). *The Purple Guide to Health, Safety and Welfare at Music and Other Events*. EIF Ltd, Chepstow: UK. Retrieved on June 22nd 2022, URL: <https://www.thepurpleguide.co.uk/index.php/the-purple-guide>

⁴⁰ ProSPeReS Project (2022). *D 2.1 - Manual for vulnerability assessment. Regional stakeholders in the protection of public spaces*.

Assessment Checklist (VAC), combined with the EU Quick Guide⁴¹ for the protection of PW, elaborated by DG HOME.

In general, a Vulnerability Assessment is a process used to define, identify, classify and prioritize vulnerabilities to attacks that stem from several factors such as the aforementioned high concentration of people combined with a lack of security measures. Vulnerability assessments also provide the organisation doing the assessment with the necessary knowledge, awareness, and risk backgrounds to understand and react to threats. A comprehensive vulnerability assessment, along with a management programme can help stakeholders improve the protection of their spaces by adopting focused and justified security measures and policies, and thus make better-informed decisions. The identification of vulnerabilities should be based on current security measures and PW effectiveness to mitigate or manage potential threats.

If you are interested in more complete, accurate information related to this, go to “VAT Lite”, by scanning the QR-code or using the link below.

<https://prosperes.eu/resources/>



The stakeholders involved in the management, protection, safety, and security of places of worship should implement appropriate practices (such as using the VAT Lite to help better protect their PW) in order to be aware of these locations' vulnerabilities to potential attacks. This would improve their ability to identify and adopt prevention and mitigation measures against attacks such as terrorist attacks, and implement appropriate practices based on the assessed likelihood and consequences of such threats.

The use of VAT Lite aims to provide a solid basis for a wider risk assessment process of a specific site/place. Based on the EU VAC, the VAT Lite is meant to serve as quick and easily understandable form of the originally produced EU VAC for public spaces that are generally considered open and accessible to members of the public. Examples of public spaces that can use either the Secu4All Quick VAT for all public spaces include transport hubs, cultural venues, business venues, parks, and other types of public spaces where many people gather or pass through. The VAT Lite however has been specifically designed for Places of Worship or for the protection of ancient buildings, due to their unique constructions. The goal of the VAT Lite, and in general of vulnerability assessments, is for a managing body of a specific type of building or public space, to be able to identify and analyse possible risks to their public space and more importantly, to mitigate the risks. The mitigation of risks can be done in several ways, which for PW specifically, can be found in ProSPeReS materials.

This process of (learning how to start) better protecting public space, has been described the ISO Risk Management Guidelines in four easy steps (see below).

⁴¹ European Commission (2021). EU Quick Guide to support the protection of Places of Worship. Retrieved on July 22nd 2022. URL: https://home-affairs.ec.europa.eu/document/download/8a4ef2e6-12ff-446d-9df5-1ce164adab25_en?filename=EU%20Quick%20Guide%20to%20support%20protection%20of%20Places%20of%20Worship_en.pdf

Figure 9 – Risk Assessment process⁴²



The basic four step programme helps you to walk through the most important steps of identifying and solving possible treats to the security of your PW and the safety of the worshippers.

- **Step 1: Risk identification.** Identify possible risks, such as a possible vehicle attack, bladed weapons attack, firearms attack or CBRN-attack.
- **Step 2: Risk analysis.** To analyse the risks (for instance: how do I check if a firearms attack will actually take place?), is it important to understand two things. **1) What is the probability** of such an attack occurring? Are there any signs? Did anyone in the community mention someone forming a potential radicalized individual? And if such an attack would occur, how severe would the **2) consequences** then be?

Figure 10 – Risk Matrix for risk analysis

		PROBABILITY / LIKELIHOOD				
		Very Low (Insignificant)	Low (Minor)	Medium (Moderate)	High (Major)	Very High (Extensive)
CONSEQUENCES	Very Low (Insignificant)	Very Low	Very Low	Low	Medium	Medium
	Low (Minor)	Very Low	Low	Medium	Medium	High
	Medium (Moderate)	Low	Medium	Medium	High	High
	High (Major)	Medium	Medium	High	High	Very High
	Very High (Extensive)	Medium	High	High	Very High	Very High

⁴² ProSPeReS Project (2022). D 3.1 – Analysis and assessment of the relevance of state-of-the-art measures taken to protect public places. Risk assessment process.

Very Low/Low:

is not considered a vulnerability. e.g., the attack can be mitigated by existing security measures.

Medium:

is considered a vulnerability. e.g., the attack cannot be mitigated by existing security measures and should be mitigated by the managing body and its partners.

High/Very High:

is considered a critical vulnerability. e.g., the risk cannot be mitigated by measures that the municipality and its partners can manage themselves.

Table 5 – Risk criteria

Consequences	Probability
Crowd density	Access to weapons
Proximity to the main site (P5)	Attractiveness of phase
Existing security measures	Crowd density
Type of weapon used	Ease of access to the site
Fatalities	Ease of escape
Physical damage	Existing security
	Past incidents

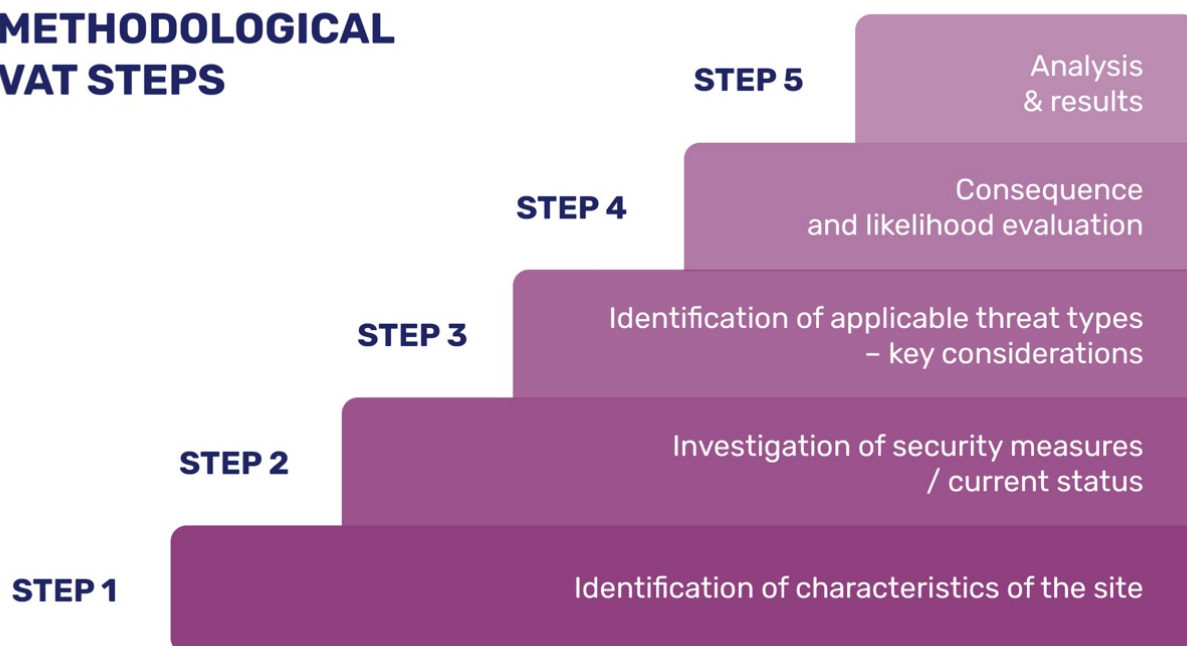
Please check the risk factors.

- **Step 3: Risk Evaluation.** Make sure that before you actually decide on the outcome, you have a discussion with staff members and if possible some experts on the risk evaluation criteria. For instance, which level of risk is acceptable to you? At what level of risk do you start to think about incorporating accurate measures or asking for help of professionals that are experts in risk mitigation?
- **Step 4: Risk treatment.** Find ways to limit possible risks, based on the checklist you can find in the ProSPeReS VAT Lite for instance.

As stated above, it is easy to create procedures and check the security level of your place of worship in accordance with your existing procedures. To keep it simple, please follow the ProSPeReS procedures, methodology and tools designed to cope with the requirements and capacities of the places of worship.

Figure 11 – Methodological VAT steps – ProSPeReS

METHODOLOGICAL VAT STEPS



If you are interested in more complete, accurate information related to the official XL version of the VAT Lite (the Vulnerability Assessment Checklist), go to “D 2.1. Manual for Vulnerability Assessment”, by scanning the QR-code or using the link below.

<https://prosperes.eu/resources/>



Prevention against attacks at technical and equipment levels.

In this subsection you will learn how prevent attacks on places of worship through the use of equipment and technical solutions. Please, consider what you can apply or change at your place of worship based on the information below.

“Appendix 2 – Recommendations for equipment to use for monitoring, detection, and protection” provides information about facility security measures such as:

Area 1 – External premises of the facility

- Anti-intrusion barriers
- Anti-ramming barriers
- Bollards
- The anti-terrorism vehicle barriers.
- Portable temporary roadblocks.
- Gates
- Security post
- CCTV system

Area 2 – Facility entry points

- Unauthorized opening of doors and windows alarm system
- Interlocking door systems
- Access control (e.g.: Biometric Access Control, Radio-Frequency Identification (RFID), Pin Code Access Control Systems)
- Turnstile gates
- Signage
- Façade
- Doors, glazing and windows
- Screening and detection equipment (e.g.: Handheld Metal Detectors, Walk-through metal detectors)
- X-Ray scanners
- Explosives detectors
- CBR detectors

Area 3 – Internal zone

- Safe room
- Mailroom
- Ventilation system
- Control room
- Water supply
- Emergency power supply

If you are interested in more complete, accurate information related to this, go to “Appendix 2 – Recommendations for equipment to use for monitoring, detection and protection”, by scanning the QR-code or using the link below.

<https://prosperes.eu/resources/>



4.2. Protection

Protection – is one of the ways to reduce the vulnerability of public spaces and critical infrastructure. The EU pays special attention to the protection of public places, particularly the sensitive ones - "soft targets", dedicating many activities, projects, and solutions to increase the safety & security of users/people. In this context, we can also observe a significant interest in protecting places of worship.

Protection zones are:

- the peripheral zone of facility protection,
- the area whose internal boundaries are the boundaries of the protected facility; the internal zone of protection of an object is the area inside the buildings that constitutes the object.
- the external boundaries defined on an ad hoc basis depending on the needs (e.g. the number of worshippers taking part in the event). The external zone of protection of an object is the area whose external borders constitute the boundaries of the area where the object or complex of objects is located (e.g. a building, a chapel, a basilica, a dwelling house).

Places of worship protection is a term close to prevention. It can be understood as coherent and planned activities related to the organisation of PW (procedures, equipment, infrastructure, personnel) and the implementation of security systems (CCTV, anti-intruder systems, access control, etc.) to protect people from attacks and to protect property.

In the previous section entitled "Prevention", you were given suggestions for preventive measures can be taken to increase the security level of your place of worship.

The following section offers suggestions on how to increase the "Protection" level of a PW.

You are advised to pay attention to the following:

- The adequacy of the PREVENTION security level at a place of worship has a direct impact on its PROTECTION level.
- Many aspects of organizing PREVENTION are developed and replicated at the PROTECTION stage,
- The authors of the Guidebook ask users to familiarize themselves with the materials from the PREVENTION subsection before reading the PROTECTION section.
- For the purposes of this manual, the elements described in the previous subsection will not be repeated.
- The section concerning PROTECTION will only describe additional elements not mentioned previously or essential items.

For assured high-level PROTECTION at your place of religious worship, the following steps are recommended:

1. Building relationships as part of multi-stakeholder and community cooperation
(Please, read Chapter 3)
2. Introduce all possible solutions related to PREVENTION
(Please, read Chapters 4 and 4.1.)
3. Introduction of the following recommendations:

To PROTECT your place of worship

The suggestions for “Security by Design” solutions are presented in chapter 4.1. PREVENTION. They also meet the criteria for PROTECTION solutions.

If you are interested in more complete, accurate information related to this, go to “Appendix 1 – Set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks”, by scanning the QR-code or using the link below.

<https://prosperes.eu/resources/>



Architectural and organisational aspects ensure an appropriate level of PROTECTION.

If the correct organisational solutions are put into action at your place of worship and complemented with architectural solutions, you will have an efficient system that provides the high level of PROTECTION your place of worship requires.

In addition to being incorporated into the design, architectural elements can also be used selectively to complement the PROTECTION of the existing structure. All necessary information is available in the “D 3.2. Security by Design Guidebook for Religious Sites” where you will find detailed and practical information on how to:

1. Establish Separate Zones.
2. Define a Public Area.
3. Establish a Restricted Area.
4. Define Border between Zones.
5. Establish a Dedicated Area.
6. Establish Access Control.
7. Define Authorized Personnel.
8. Establish Access Control Between a PW and its External Surroundings.
9. Establish Access Control to a Restricted Area.
10. Establish Evacuation Routes and Exits.

How to implement physical and technical PROTECTION

If you are interested in more complete, accurate information related to this, go to “Appendix 2 – Recommendations for equipment – monitoring, detection and protection”, by scanning the QR-code or using the link below.

<https://prosperes.eu/resources/>



In the “D3.2. Security by Design Guidebook for Religious Sites”, “Appendix 2 – Recommendations for equipment – monitoring, detection, and protection” and “Appendix 1 – Set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks” you will find detailed and practical information on how to:

1. Employ a security company, or private security consultant or train volunteers.
2. Engage Volunteers/Staff.

Use technical equipment to PROTECT your place of worship

Subsection 4.1. PREVENTION, contains various technical solutions that enhance the safety of places of worship. These solutions also raise the PROTECTION level of places of worship so we encourage you as the user to familiarize yourself with the described in section 4.1. Below, you will find some other recommendations especially selected to increase the PROTECTION level of PW.

Protecting religious facilities, their staff, and worshippers is a great challenge, which must combine all the elements necessary for everything to function properly and not be an inconvenience to the people visiting the temple.

An appropriate and comprehensive approach to this topic often represents a substantial financial investment. This study serves as a guideline for solutions used in public buildings as a suggestion for existing applications. Not all of these solutions can be applied to every place, however, they can be a guideline to which equipment applications should be directed.

Malfunctions or inadequate preparation of a building’s security system can expose the facility to many different hazards and risks, ranging from theft to the worst-case scenario of a successful terrorist attack. A poorly designed access control system makes it much easier to launch such attacks.

One of the critical goals of the multi-level protection concept is the comprehensive implementation of security measures that integrate physical, technological, and operational standards.

From a technical standpoint, crucial factors must be covered to ensure the safety of congregation members arriving at places of worship.

The facility should be divided into several areas of interest to approach this problem comprehensively.

The adaptation of technical protection systems should be tailored individually to the specific facility’s needs and preceded by a specialized security audit.

The first source of information regarding enhancing security at a facility should be the local Law Enforcement Agencies (LEAs) responsible for conducting operations in the particular area in which the facility is located. Cooperation with the police is particularly important with regard to updating the threat level on a daily basis and during preparation, as well as protection of an ongoing event, expert advice on procedures, and special equipment recommendations. Due to its broad, specialized expertise in

countering terrorist threats, it is a source of valuable information and support during the organisation of events that gather large numbers of people together.

Types and levels of threats

The following recommendations are intended to serve as a guide to identify ways to eliminate gaps in a facility's security system to combat given types and levels of threats. They are divided into ones covering the facility and its infrastructure and ones covering personnel. Any effort to equip the facility and personnel with appropriate technical measures should be preceded by a professional assessment of the facility's security and safety measures following expert advice to adapt them to meet the current levels and types of threats.

Due to the complexity of the problem of making equipment recommendations, they have been divided into three types of threats:

1. General terrorist acts (GENERAL).

This group includes other terrorist attacks unrelated to IED and CBRN threats. These include but are not limited to the following:

- Sharp object attack,
- Firearms attack,
- Hand grenades/projectiles attack,
- Vehicle attack,
- Incendiary,
- Hostage-taking,
- Kidnapping.

2. Improvised explosive device (IED).

IED threats include one or more incidents involving improvised explosive devices, such as:

- IED detonation,
- Explosion,
- Find,
- Hoax,
- False,
- Turned-In.

3. CBRN.

Incidents include all threats involving the use of CBR agents, regardless of whether they are triggered intentionally or unintentionally.

Intentional - CBRN incidents that involve the intentional release by states, non-state armed groups, terrorists, or criminals, with the intent to cause injury and death, cause fear and panic in individuals or a specific group of the local population.

Non-intentional - events related to industrial accidents, accidents in military research centres, related to accidents during the transportation of hazardous goods, natural sources of infection with bacteria or viruses, natural disasters leading to the destruction of industrial or military installations, and remnants of war.

However, this does not mean that every terrorist attack uses only one type of threat. Current trends indicate that terrorists are aiming for complex attacks, using all types of available weapons (firearms, bladed weapons, hand grenades, IEDs to CBR agents). Therefore, in the comprehensive preparation of a facility against terrorist attacks, all types of threats should be considered and implemented in security plans, technical upgrades, and individual equipment.

For the purposes of equipment recommendations for PW, the risk level for a given threat is determined based on the VAT light (Vulnerability Assessment Tool light), resulting from the assessed probabilities and consequences of threats.

The recommendations are expressed in the form of a table. The table is a pre-set tool designed to indicate minimum equipment recommendations based on the identified type of threat and its level.

If you are interested in more complete, accurate information related to this, go to “Appendix 2 – Recommendations for equipment – monitoring, detection and protection”, by scanning the QR-code or using the link below.

<https://prosperes.eu/resources/>



There you will find detailed and practical information on, among others:

1. CCTV,
2. Anti-stabbing vests,
3. Bullet and fragmentation-resistant vests.

4.3. Detection

Detection – in terms of terrorism, detection is the ability to detect early terrorist threats, objects, and substances of concern, and terrorists, especially by using recent technologies. In order to detect terrorist threats in places of worship, it is important to inform religious communities that gather in these places how to properly identify threats, report suspicious behaviour or objects, and raise awareness of these communities as well as give patterns of reactions in the event of terrorist threats.

The previous sections, 4.1. "Prevention" and 4.2. "Protection", contain suggestions for preventive measures that can be taken to increase the security level at your place of worship.

The following section offers suggestions on how to increase the "Detection" level of any threats against your PW.

The authors of the handbook ask you, dear User, to pay attention to the following:

- The adequacy of the PREVENTION and PROTECTION security measures taken at the place of worship has a direct impact on the DETECTION level.
- Many aspects of organizing DETECTION are developed and replicated at the PREVENTION and PROTECTION stage.
- Please familiarize yourself with the materials in subsections 4.1. PREVENTION and 4.2. PROTECTION before reading the DETECTION section.
- For the purposes of this manual, in this subsection, the elements described in the previous subsection will not be repeated.
- In the DETECTION section, only additional elements not previously mentioned or those that are so important they must be reintroduced will be described.

Picture 11 – The moment of detection of an unattended backpack



To increase the threat detection rate at your place of religious worship, we suggest:

Please, read Chapter 3 – building relationships as part of multi-stakeholder and community cooperation. It is very important to create a comprehensive system for observing and informing about possible threats.

Please remember:

Information received from outsiders should never be ignored or underestimated. They may be neighbours who do not follow our religion, but this does not mean that as people, they do not care about the safety of their neighbourhood. Building relationships with all players based on our mutual concern for the safety of our neighbourhood and district can lead to a more concerted and effective effort towards the protection of the area.

Please, read Chapter 4: 4.1. PREVENTION, 4.2. PROTECTION – introducing all possible solutions related to PREVENTION and PROTECTION strongly influences the ability to detect and reveal threats.

It is especially worth paying attention to the importance of detecting possible preparations for an attack or its initiation with the help of:

- stakeholders, neighbours
- employees, staff
- trained volunteers
- CCTV operators and CCTV system
- security company, security staff
- private security consultants

If you are interested in complete, accurate information related to this, go to “Appendix 2 – Recommendations for equipment – monitoring, detection, and protection” for detailed and practical information on, among others:

1. CCTV fitted with a facial and behavioural recognition system
2. Left item detection
3. Body Worn Camera (Bodycam)
4. Radio communication system
5. Drone solutions

4.4. Response

Response – in terms of terrorism, at the EU level is to ensure having a legal framework to act, making most of the operational support given by EU’s agencies (Europol and Eurojust), ensuring that victims are supported and protected⁴³.

To better respond to terrorist threats identified against places of religious worship in the European Union, activities are undertaken to build systemic solutions, combining resources, services, and religious communities for a coherent and effective response to the threat, limiting casualties and losses.

Previous sections: 4.1. "Prevention," 4.2. "Protection" and 4.3. "Detection", contain suggestions for preventive measures that can be taken to increase the security level of your place of worship.

The following section considers ways you may respond to threats and attacks.

Focus points to bear in mind include:

- Good PREVENTION, PROTECTION, and DETECTION security levels at the place of worship have a direct impact on RESPONSE capabilities.
- The RESPONSE level is reinforced by correctly implemented and applied recommendations, which the authors of the guidebook described in 4.1. "Prevention", 4.2. "Protection" and 4.3. "Detection". You are advised to read these sections before reading 4.4 "Response".
- All the procedures should be implemented in accordance with any national laws and respect any regional or local regulations or conditions that may be different in some Member States.
- The overall emphasis of the procedures can be illustrated as follows:

Figure 12 – Procedures alignment to security objectives



Source: Appendix 1 – Set of procedures to prevent, protect, detect, respond to and mitigate the results of terrorist attacks - procedures alignment to security objectives.

⁴³ European Commission, *A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond*, p. 2.

If you are interested in complete, accurate information related to this, go to “Appendix 1 – Set of procedures to prevent, protect, detect, respond to and mitigate the results of terrorist attacks”. You will find, among others, detailed procedures and information about the following:

1. GUIDE for incident managers of terrorist/extremist threats and attacks.
2. GUIDE for interoperability with the emergency services.
3. GUIDE for developing a Welcome Team.
4. ADVICE for the public to stay safe during a terrorist/extremist attack.
5. ADVICE for the public to stay safe during a CBRN incident.
6. ACTIONS to take IMMEDIATELY following a CBRN incident.
7. OPTIONS for the emergency response to a terrorist/extremist threat or attack.
8. GUIDE for evacuation planning.
9. GUIDE for invacuation planning.
10. GUIDE for lockdown planning.
11. ACTIONS to take when a suspicious item of mail, package, substance is discovered.
12. ACTIONS to take if a bomb threat-hoax is received.
13. ACTIONS to take when a suspicious item is discovered.
14. CHECKING your venue for suspicious items.

If you are interested in more complete, accurate information related to this, go to “Appendix 1 – Set of procedures to prevent, protect, detect, respond to and mitigate the results of terrorist attacks”, by scanning the QR-code or using the link below.

<https://prosperes.eu/resources/>



4.5. Mitigation of the results of terrorist attacks

Mitigation of the results of terrorist attacks for the purpose of this guidebook is the proper response after the terrorist attack to minimize its impact and make sure that investigation and prosecution of the terrorists are taken as fast as possible⁴⁴.

Previous sections 4.1. "Prevention", 4.2. "Protection", 4.3. "Detection" and 4.4. "Response", offer suggestions for preventive actions that can be taken to increase the security level of your place of worship.

The following section has suggestions on how to MITIGATE the results of terrorist attacks.

⁴⁴ European Commission, *A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond*, p. 14

The authors of the Guidebook ask users to pay attention to the following:

- good PREVENTION, PROTECTION and DETECTION security level of the place of worship has a direct impact on your capacity/ability to MITIGATE the results of any attacks,
- RESPONSE procedures and RESPONSE reactions have a direct impact on your capacity to MITIGATE the results of any attacks,
- the Mitigation of the results of terrorist attacks is reinforced by correctly implemented and applied recommendations, which the authors of the guidebook described in 4.1. "Prevention", 4.2. "Protection", 4.3. "Detection" and 4.4. "Response". If you have not read these sections, you are advised to do so before reading the section below.

If you are interested in more complete, accurate information related to this, go to "Appendix 1 – Set of procedures to prevent, protect, detect, respond to and mitigate the results of terrorist attacks", by scanning the QR-code or using the link below.

<https://prosperes.eu/resources/>



Unfortunately, even if the recommendations made in previous sections are considered and applied, a terrorist attack may still occur.

Of course, it goes without saying that if you are engaged in mitigating the results of an attack, this means that an attack has already taken place.

There is probably damage and maybe injured or possibly even dead people.

Despite this, there are VERY IMPORTANT things that can be done even at this late stage to limit the negative impact of an attack.

An attack will usually cause chaos and panic so it is vital to focus on the following points:

1. **Cooperation with emergency and security services.**
2. **Continue evacuation from risk area (support emergency and security services).**
3. **Give first aid and medical treatment to the victims of the attack.**

Figure 13 – Reminder of the importance of first aid



Despite the stress and chaos caused by an attack, it is of the utmost importance that victims receive first aid as quickly as possible. Whether in everyday life or after an attack, the quick reaction of witnesses to an accident or attack is crucial.

Emergency services will usually reach the injured within 10-15 minutes. In a post-attack situation, this time may be extended.

Pre-medical assistance provided by people at the scene of the incident is of great importance.

Picture 12 – Giving first aid to a victim of an attack



Massive bleeding from a damaged artery usually causes the victim to bleed out within 2 MINUTES. Therefore, applying hand pressure or a tourniquet to the wound as soon as possible is crucial. Most often, these two minutes determine whether a casualty lives or dies.

Resuscitation of a person in cardiac arrest within 4-5 MINUTES is usually successful. The use of an AED defibrillator or heart massage is vital.

Section 3.4. Recommendations for monitoring, detection and protection equipment, provides, among other things, detailed information about:

- AED kits;
- Tourniquets;
- Burn dressings;
- Hemostatic dressings;
- Emergency kits.

Cooperation with security services during an investigation

Provide secured CCTV materials and share your observations with law enforcement officers. For example, your assumptions, and any information that may explain the causes or reveal the perpetrators of the attack and their associates and provide evidence during a possible criminal trial.

You can save many lives:

Please remember that by cooperating with security services, you can save many lives. It's possible that the attack on your place of worship was one of many planned. Your cooperation with the authorities may prevent further attacks and bring the perpetrators to justice.

Organize PTSD (Post Traumatic Stress Disorder) support for victims and witnesses

As evidenced by psychological research and experiences from past attacks, both WITNESSES AND VICTIMS of an attack are at risk of developing PTSD or other anxiety-depressive states.

The religious community is based on mutual trust and assistance. Therefore, after an attack on a place of worship, you can still help the event participants. This is all the more true because often victims may only start to display the first symptoms of PTSD or other traumas caused by an attack several weeks or months after the event.

Surrounding your faithful with additional care and watching for signs of problems like neuroses, anxiety, alcohol abuse, or a sudden deterioration of interpersonal relationships is important so that sufferers can be persuaded to get specialized psychiatric or psychological help.

Please remember that anybody involved in a terrorist attack, both witnesses and victims, can suffer from the after-effects of such (possible) trauma⁴⁵. Also be aware of the fact that some individuals might not necessarily feel traumatized per se and that by labelling them as "traumatized", you can also cause psychological damage to individuals.

⁴⁵ Bosmans MWG, Plevier C, Schutz F, Stene LE, Yzermans CJ and Dückers MLA (2022) The impact of a terrorist attack: Survivors' health, functioning and need for support following the 2019 Utrecht tram shooting 6 and 18 months post-attack. *Front. Psychol.* 13:981280. doi: 10.3389/fpsyg.2022.981280

5. General idea of awareness and training

An important component of activities designed to strengthen the resilience of a religious community and its facilities to terrorist attacks or violent extremism will pay sufficient attention to issues related to raising the awareness of worshipers, clergy, staff, etc. Training them to prevent attacks and, in the event of an attack, how to survive it and limit casualties and other losses can be very advantageous. Other specialized forms of training using the latest technologies should be directed towards people responsible for the security of religious assemblies, etc.

As part of the ProSPeReS project, experts have created a set of specially prepared training sessions aimed at groups of people related to PW activities. Below is a general outline of the topics professionally presented in training modules available to the relevant representatives of religious communities.

Figure 14 – Related word cloud



Table 6 – Outline topics

THEORETICAL PART	Analysis of the current state of threats to PW	Importance of and need for the protection of religious sites in the EU in light of radicalization and violent extremism
		Terrorist threats in Europe. General trends and methods (e.g. car ramming, firearms, IED)
		Attacks on PW – perpetrators, methods and victims
		Characteristics of various places of worship and large gatherings of people – vulnerability and resilience
	Strategies for counteracting threats to the PW – the EU dimension	Preventing and counteracting terrorism in the EU Member States’ legal framework - the community dimension
		Security by Design for PW
		Risk identification, analysis and evaluation
		Vulnerability assessment and tools: VAT for large gatherings and VAT lite
		Security Systems in PW (CCTV, Access Control etc.)
		The role of LEAs, Fire Dept., municipalities and private security sector
Competences and Capacities of Religious Communities / Management of PW		
PRACTICAL PART	CBRN threats	CBRN: An Introduction
		Chemical warfare agents
		Biological threats - Radiological and Nuclear threats
		Personal protection equipment and decontamination
		CBRN Scenarios with reactions models
	Procedures and practical aspects of protecting worshipers and religious sites	The practice of securing various PW (security management)
		The planning process to protect religious places and events
		Conducting protective activities regarding worshipers (daily activities and mass events)
		Equipment (PPE and other placed in the PW)
		Responding to threats - acting in a crisis - procedures, first responders, event management and crisis management
		Activities after an incident (e.g. psychological support, investigation etc.)
		Multi-institutional cooperation at local level (before, during and after an incident)

Training, and practice of the different stages: Prevention, Protection, Detection, Response, and Mitigation are crucial to increase security in a place of worship.

Properly trained:

- workers;
- staff;
- volunteers;
- welcome team;
- CCTV operators.

significantly increase the level of security in a place of worship.

Picture 13 – A safe family on community property



Successful implementation of the contents of the Guidebook depends on the extent to which the procedures, knowledge and technical expertise covering evacuation routes and basic first aid principles described are used.

The importance of the training process for the implementation of the procedures and recommendations described in previous chapters and particular deliveries is enormous. Moreover, all the theoretical information provided must be converted into training.

6. Conclusions

Terrorism, characterized by fear, the unpredictability of incidents, and the possibility of mass casualties, is a phenomenon that activates those responsible for security throughout the European Union and globally. However, the local dimension of security efforts should be emphasized, including activities at the lowest levels of administration - in direct contact with citizens. EU documents also underlined the importance of this aspect of activities for security: the EU Counter-Terrorism Agenda, research and reports developed during the ProSPeRes project, and materials of many other institutions, including EFUS - European Forum for Urban Security⁴⁶. **The ProSPeReS project on protecting religious places (organisations of the faithful, churches, mosques, synagogues, religious events) pays special attention to the community dimension of security activities and close, direct cooperation with LEAs, fire brigades, municipalities, etc.**

Legal solutions, competencies, and awareness of individual participants in the security management process should guarantee professionalism in the face of a threat. Preventing terrorism and effective response during an attack is the most important and most challenging action, relevant on the one hand for the LEAs and, on the other hand, essential for all members of the local community, including religious congregations of various denominations, which often live side by side and are constantly exposed to extremist/terrorist activity, not only in the form of an attack but also in the phase of progressive radicalization, violence, as well as planning and preparing an attack.

The abovementioned issues are of great importance for PW, which are open in nature and encourage people to engage in religious practices. These sensitive places, often without special protection, require professional actions and care of the facility managers for the safety of the faithful.

This Guidebook, touching on many issues related to PW security, is intended to be a real support for those who strive to improve the level of protection of worshipers and PW facilities as well as large gatherings of people for religious purposes. **The protective procedures indicated in the material, and those related to planning the security of the PW, as well as those about reacting in the face of an attack; proposals on security technologies for the PW and PPE equipment, as well as communication and cooperation protocols between the PW and other stakeholders, can positively change the local security environment.** The above was supplemented with a ready-to-implement, comprehensive crime prevention concept: **Security by Design** addressed to PW managers.

To sum up, it is worth paying attention to the **selected determinants of effective action against terrorism from the subjective perspective**, i.e., regarding people who may have an impact on the security of the PW:

- social (worshipers, clergy members, neighbours to the PW) and individual (individual) awareness of threats;
- preparation and high competencies (knowledge and skills) of the community to respond to symptoms of threats - anticipating them and appropriate behaviour in the event of an attack;
- readiness for positive cooperation resulting in the creation of bonds, integration, joint implementation of goals, creating a community that manages hazards;
- competencies, predispositions, and proper selection of a terrorist incident proving on the spot, resulting in good decisions and orders, which is crucial for crisis management;
- competencies of other participants in the institutional process of counteracting terrorism.

⁴⁶ More at: <https://efus.eu/>

The objective approach concerns, to a large extent, legal tools, material resources, and organisational solutions that serve to combat the phenomenon of terrorism effectively. **The most important determinants of effective action against such a threat, in terms of subject matter, are:**

- clear, transparent legal background and executive procedures, rules, and guidelines;
- good practice of coordinating activities, exchanging information, and alerting services and local society;
- unified definition (the same “language”), understanding, and perception of phenomena by participants in the process of counteracting terrorism as a source of effective joint initiatives;
- pro-active, universal, multi-agency prevention strategies;
- effective, optimizing activities and standards for the cooperation of stakeholders, including communities, public and local administration, LEAs, other services, and armed forces;
- appropriate individual and team equipment and armament of officers and soldiers, as well as equipment of other entities competent in the field of medical and technical rescue, etc.;
- low sensitivity of individual elements of the local security environment to threats;
- effective international cooperation.

Ten tips for strengthening security of PW:

1. Conduct a risk analysis assessment for the places of worship.
2. When planning a new location for a place of worship, consider the security measures detailed in the Security by Design concept.
3. Include the security awareness issue in your community's organisational culture, including its provision at management and strategic levels.
4. Ensure proper maintenance of the facility - order, lighting, free spaces, escape routes.
5. Consider the open nature of places of worship, monitor the available space, and apply access control for selected and non-public spaces.
6. Install appropriate technical security measures (locks, video surveillance, motion sensors, lighting).
7. Check the security of deliveries and mail.
8. When recruiting employees or contracting services, check personal data and references.
9. Consider how best to secure places of worship's data, including its information systems.
10. Plan proper behaviours / procedures in a crisis.

Source: ProSPeReS research based on materials from www.cpni.gov.uk

Finally, hope that the presented guidance and solutions will be interesting and valuable for Guidebook users. **The practical implementation of the procedures will be highly dependent on the following factors:**

- adequate training for the staff, including regular drills, rehearsals, and exercises involving the procedures;
- awareness among staff and worshipers;
- capabilities and resources to implement security technologies;
- cooperation with LEAs, public services, municipalities, and key stakeholders;
- joint planning and interoperability with LEAs.

At the same time, it should be emphasized that all procedures should be considered in the context of national laws. Any regional or local regulations or conditions that may differ in some Member States must be respected. Furthermore, consider the capabilities of relevant public services and guidance available, especially from law enforcement agencies. If you identify a potential or real serious threat, contacting the police (or other LEAs) will be necessary.

7. List of tables, figures and pictures

Tables

Table 1 – Abbreviations used in the document.....	6
Table 2 – Definitions used in the document.....	8
Table 3 – Public spaces categories presenting soft target characteristics. D 2.1 - Manual for vulnerability assessment.....	13
Table 4 – Potential considered threats	42
Table 5 – Risk criteria	49
Table 6 – Outline topics	65

Figures

Figure 1 – Actions based on the EU Counter Terrorism Agenda.....	12
Figure 2 – Map of terrorist attacks in Europe in 2020	17
Figure 3 – Number of terrorist attacks in Europe 2019 - 2021	18
Figure 4 – Map of surveyed places of worship	24
Figure 5 – Threat types.....	26
Figure 6 – Recommendations.....	40
Figure 7 – Community cooperation.....	45
Figure 8 – State-of-the-art public spaces protection	46
Figure 9 – Risk Assessment process.....	48
Figure 10 – Risk Matrix for risk analysis	48
Figure 11 – Methodological VAT steps – ProSPeReS.....	50
Figure 12 – Procedures alignment to security objectives	59
Figure 13 – Reminder of the importance of first aid.....	61
Figure 14 – Related word cloud	64

Pictures

Picture 1 – Gathering by a place of worship (Rafał Kowalczyk based on © DisobeyArt, Adobe Stock)	11
Picture 2 – Police on duty (© Stephen, Adobe Stock)	15
Picture 3 – Large gathering (Rafał Kowalczyk based on © rparys, Adobe Stock)	23
Picture 4 – Diverse religious community (Rafał Kowalczyk based on photos taken by Rafał Batkowski).....	27
Picture 5 – Security staff on duty (© Nick Beer, Adobe Stock)	31
Picture 6 – Crisis team figuring out a plan (Rafał Kowalczyk based on © Syda Productions, Adobe Stock)	34
Picture 7 – Checking the security list (Rafał Kowalczyk based on © deagreez and © Iakov Kalinin, Adobe Stock)	37
Picture 8 – Architectural element: pots and flowerbeds in front of Agios Dimitrios Temple in Thessaloniki (Picture taken by Adrian Siadkowski).....	41
Picture 9 – Bollards (Rafał Kowalczyk based on © eranicle and © AVD, Adobe Stock).....	43
Picture 10 – Policewoman helping pilgrims (© Andrzej Mitura, Policja 997).....	44
Picture 11 – The moment of detection of an unattended backpack (Rafał Kowalczyk based on © ange1011, Adobe Stock)	57
Picture 12 – Giving first aid to a victim of an attack (Rafał Kowalczyk based on © New Africa, Adobe Stock)	62
Picture 13 – A safe family on community property (Rafał Kowalczyk based on © Валерий Зотьев, Adobe Stock).....	66

8. List of appendices

- Appendix 1 – A set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks
- Appendix 2 – Recommendations for equipment: monitoring / detection / protection
- Appendix 3 – The protocols for communication and cooperation with public services
- Appendix 4 – VAT Lite
- Appendix 5 – The Ten Rules
- Appendix 6 – Security Routine Checklist

9. References

A list of references:

- European Commission (2020). *Protection of Public Spaces Newsletter (22 April 2020): "Terrorism Risk Assessment of Public Spaces for Practitioners"*. Retrieved on July 7th, 2022. URL: [https://ec.europa.eu/newsroom/pps/item-detail.cfm?item_id=674909&utm_source=pps_newsroom&utm_medium=Website&utm_campaign=pps&utm_content=Terrorism%](https://ec.europa.eu/newsroom/pps/item-detail.cfm?item_id=674909&utm_source=pps_newsroom&utm_medium=Website&utm_campaign=pps&utm_content=Terrorism%20)
- European Council (2022). *EU measures to prevent radicalization*. Retrieved on July 7th, 2022. URL: <https://www.consilium.europa.eu/en/policies/fight-against-terrorism/preventing-radicalisation/>.
- Europol (2016). *Changes in Modus Operandi of IS revisited*,. Retrieved on July 20th, 2022. URL: <https://www.europol.europa.eu/newsroom/news/islamic-state-changing-terror-tactics-to-maintain-threat-in-europe> and Terrorism.
- Europol (2017). *European Union Situation and Trend Report (TE-SAT)*. Retrieved on July 20th, 2022. URL: <https://www.europol.europa.eu/tesat/2017/index.html>.
- Europol (2022). *European Union Situation and Trend Report (TE-SAT)* Retrieved on July 20th, 2022. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf
- OCHA (2022). *Global Terrorist Index*. Retrieved on July 20th, 2022. URL: <https://reliefweb.int/report/world/global-terrorism-index-2022>. Cambridge Dictionary (2022). *Meaning of prevention in English*. Retrieved on November 10th, 2022. URL: <https://dictionary.cambridge.org/us/dictionary/english/prevention>
- EU Commission (2020). *EU Security Union Strategy*. Retrieved on August 19th, 2022. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from=EN>
- EU Commission (2020). *A Counter Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond*. Retrieved on August 19th, 2022. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0795&from=EN>
- European Commission(2022). *Counter terrorism and radicalization*. Retrieved on July 20th, 2022. URL: https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation_en
- Council of Europe (2015). *Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism, Riga*. Retrieved on August 18th, 2022. URL: <https://rm.coe.int/168047c5ea>
- Council of Europe (2005). *Council of Europe Convention on the Prevention of Terrorism, Warsaw*. Retrieved on August 18th, 2022. URL: <https://rm.coe.int/16808c3f55>
- Council of Europe (2022). *Full list of Conventions*. Retrieved on August 18th, 2022. URL: <https://www.coe.int/en/web/conventions/full-list/-/conventions/>, (access: 18.08.2022)
- International Organisation for Standardization (2018). *ISO 31000:2018 – Risk management - Guidelines*. p.11. Retrieved on August 11th, 2022. URL: <https://www.iso.org/standard/65694.html>

- International Organisation for Standardization (2021). ISO 22341: 2021 – Security and resilience – Protective Security – Guidelines for crime prevention through environmental design. Retrieved on August 11th, 2022. URL: <https://www.iso.org/standard/50078.html>
- Oxford Learner's Dictionary (2022). "Detect". Retrieved on November 11th, 2022. URL: <https://www.oxfordlearnersdictionaries.com/definition/english/detect?q=detect>,
- Oxford Learner's Dictionary (2022). "Protect". Retrieved on November 11th, 2022. URL: <https://www.oxfordlearnersdictionaries.com/definition/english/protect>
- UNODC (2022). Tertiary, Counter-Terrorism, Module 5: Regional Counter-Terrorism Approaches, Key Issues, European Region. Retrieved on August 18th, 2022. URL: <https://www.unodc.org/e4j/zh/terrorism/module-5/key-issues/european-region.html>
- Vision of Humanity (2022). GTI 2022 MEASURING THE IMPACT OF TERRORISM. Retrieved on August 18th, 2022. URL: <https://www.visionofhumanity.org/wp-content/uploads/2022/03/GTI-2022-web-04112022.pdf>, (access: 18.08.2022)
- Batkowski, R. (2015). Counteracting asymmetric and hybrid threats from the police perspective [in:] Jałoszynski, K. et al. (red.), Police special forces in Poland, p.263.
- European Commission (2017). The European Union (EU) Action plan to support protection of public spaces. p.2. Retrieved on July 20th, 2022. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0612>
- European Commission (2017). The EU Security Union Strategy 2020-2025. Retrieved on July 20th, 2022. URL: <https://commission.europa.eu/system/files/2017-07/communication-equal-opportunities-diversity-inclusion-2017.pdf>
- PRoTECT project (2021). Public Resilience Using Technology To Counter Terrorism Project, p. 8-10. Retrieved on July 20th, 2022. URL: https://protect-cities.eu/wp-content/uploads/2021/02/PRoTECT_Deliverable-2.1-Manual-EU-VAT_v2.0.pdf
- United Nations Office on Drugs and Crime (2018). Module 5. Counter Terrorism Approaches; the European Union. Retrieved on January 3rd, 2023. URL: <https://www.unodc.org/e4j/zh/terrorism/module-5/key-issues/european-region.html>Food,
- Events and Things (2022). The Purple Guide to Health, Safety and Welfare at Music and Other Events. EIF Ltd, Chepstow: UK. Retrieved on June 22nd 2022, URL: <https://www.thepurpleguide.co.uk/index.php/the-purple-guide>



prosperes.eu



This project is funded by the European Union's
Internal Security Fund – Police under Grant
Agreement No. 101034230 – ProSPeReS



A set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks

Appendix 1

of GUIDEBOOK on security measures
for religious sites & communities

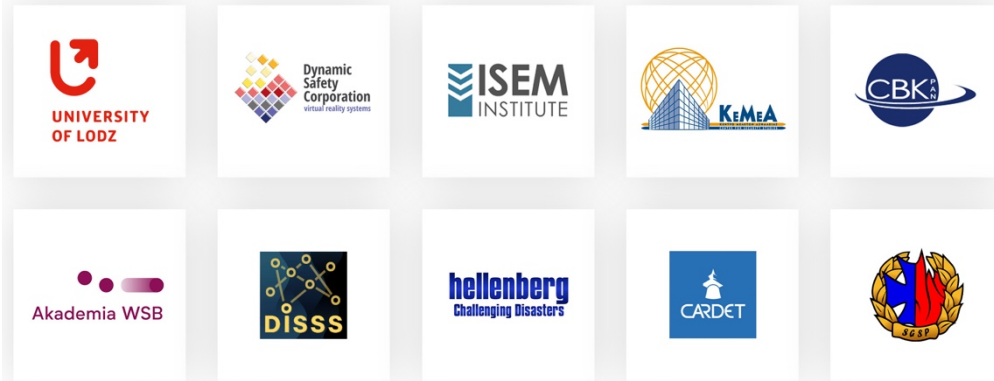


This project is funded by the European Union's
Internal Security Fund – Police under Grant
Agreement No. 101034230 – ProSPeReS

prosperes.eu

ProSPeReS consortium

Security experts, security research and academic institutions,
providers of technical solutions and services



Law enforcement agencies (LEAs)



Faith-based organizations



A set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks

Appendix 1
of GUIDEBOOK on security measures
for religious sites & communities

Document description

WP number and title	WP3 – Preparing the tailor-made security measures for religious sites. A3.3 – Preparing the set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks.
Lead Beneficiary/Author(s)	ISEMI (Cameron Mann, Pavel Truchly)
Contributor(s)/Author(s)	UL, DSC, ISEMI, WSB, DISSS, HELLENBERG, CARDET, Archdioce. Lodz, Social Obser., HMI, GWZ Warsaw, KWP Lodz, KSP, KWP Wroclaw, HELLENIC POLICE, CBK PAN, SGSP
Document type	Report
Last Update	08/03/2023
Dissemination level	Public / Confidential *

* Confidential – only for members of the consortium & EC Services

Acknowledgement:

This project is funded by the European Union's Internal Security Fund — Police. Grant Agreement No. 101034230 — ProSPeReS

Disclaimer:

The content of this document 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.



This work is licensed under the Creative Commons Attribution 4.0 International Licence. To view a copy of this license, visit creativecommons.org/licenses/by/4.0/ with relevant national copyright provisions to be applied accordingly.

The material for this publication was developed and reviewed by ProSPeReS consortium:

No	Partner organization name	Short Name	Country
1	UNIVERSITY OF LODZ	UL	PL
2	DYNAMIC SAFETY CORPORATION	DSC	PL
3	INTERNATIONAL SECURITY AND EMERGENCY MANAGEMENT INSTITUTE	ISEMI	SK
4	CENTER FOR SECURITY STUDIES	KEMEA	GR
5	WSB ACADEMY	WSB	PL
6	STICHTING DUTCH INSTITUTE FOR SAFE AND SECURE SPACE	DISSS	NL
7	HELLENBERG INTERNATIONAL	HELLENBERG	FI
8	CENTRE FOR THE ADVANCEMENT OF RESEARCH & DEVELOPMENT IN EDUCATIONAL TECHNOLOGY LIMITED	CARDET	CY
9	ARCHDIOCESE OF LODZ	Archdiocese Lodz	PL
10	SOCIAL OBSERVATORY FOUNDATION	Social Obser.	PL
11	HOLY METROPOLIS OF IOANNINA	HMI	GR
12	JEWISH COMMUNITY OF WARSAW	GWZ Warsaw	PL
13	LODZ VOIVODESHIP POLICE	KWP Lodz	PL
14	WARSAW METROPOLITAN POLICE	KSP	PL
15	WROCLAW VOIVODESHIP POLICE	KWP Wroclaw	PL
16	HELLENIC POLICE	HP	GR
17	SPACE RESEARCH CENTRE POLISH ACADEMY OF SCIENCE	CBK PAN	PL
18	THE MAIN SCHOOL OF FIRE SERVICE	SGSP	PL

Table of Contents

Table of Figures	8
Introduction	9
1. GUIDE for incident managers of terrorist/extremist threats and attacks	12
1.1. MAKE a first assessment:	13
1.2. INFORM emergency services	13
1.3. DECIDE on the first actions	14
1.4. COMMUNICATE decisions and instructions	15
1.5. REVIEW the situation	15
1.6. MAINTAIN a record	15
1.7. Personal Training	16
2. GUIDE for interoperability with the emergency services	18
3. GUIDE for developing a Welcome Team	20
3.1. Role of the Welcoming Team	20
3.2. Staff and/or Volunteers	20
3.3. Deployment	20
3.4. Communications	21
3.5. Training	21
4. ADVICE for the public to stay safe during a terrorist/extremist attack	22
5. ADVICE for the public to stay safe during a CBRN incident	24
6. ACTIONS to take IMMEDIATELY following a CBRN incident	25
7. OPTIONS for the emergency response to a terrorist/extremist threat or attack ...	28
7.1. No action required	28
7.2. Full Evacuation	28
7.3. Partial / Phased / Zonal Evacuation	28
7.4. Directional Evacuation	28
7.5. Invacuation	28

7.6. Full Lockdown	29
7.7. Partial / Phased / Zonal Lockdown	29
8. GUIDE for evacuation planning.....	30
9. GUIDE for invacuation planning	32
10. GUIDE for lockdown planning	34
11. ACTIONS to take when a suspicious item of mail, package, substance is discovered.....	36
12. ACTIONS to take if a bomb threat-hoax is received	38
13. ACTIONS to take when a suspicious item is discovered	42
14. CHECKING your venue for suspicious items.....	44
Conclusions	45

Table of Figures

Figure 1 – Procedures alignment to security objectives	9
Figure 2 – Steps made by incident manager	12
Figure 3 – ETHANE structure report.....	13
Figure 4 – Remove, Remove, Remove	27
Figure 5 – Suspicious letter and package	37

Introduction

This document provides a set of procedures to prevent, protect, detect, respond and mitigate the consequences of terrorist/extremist attacks at places of worship and large religious gatherings and protect the relevant stakeholders.

All the procedures should be implemented in accordance with any national laws and respect any regional or local regulations or conditions which may be different among Member States.

Concerning the overall security objectives, it was found that response and mitigation were the areas of greatest need with the largest gaps requiring procedures specifically designed and developed for places of worship and large religious gatherings. Clearly defined roles and responsibilities for a trained 'Incident Manager' and a 'Welcome Team' (security and/or volunteers) together with their 'Interoperability with Emergency Services' were considered essential for developing effective and efficient capabilities to implement the full set of procedures in an emergency situation. Concerning the security objectives of prevent, protect and detect, it was found that implementation of standard security measures could generally be relied on; these have been carefully considered and set out in the ProSPeReS 'Security by Design Guidebook'. The overall emphasis of the procedures can be illustrated as follows:

Figure 1 – Procedures alignment to security objectives

	Prevent	Protect	Detect	Respond	Mitigate
Incident Manager				█	█
Interoperability	█	█	█	█	█
Welcome Team	█	█	█	█	█
Public Advice – Terrorism				█	█
Public Advice – CBRN				█	█
CBRN			█	█	█
Tactical Options				█	█
Evacuation				█	█
Invacuation				█	█
Lockdown				█	█
Suspicious Packages			█	█	█
Bomb Threat-Hoax				█	█
Suspicious Items				█	█
Checking Premises	█	█	█	█	█

STANDARD SECURITY MEASURES

The procedures are intended for implementation acknowledging the many and various differences between places of worship concerning their security and emergency management arrangements. The set of procedures have been designed using the following principles:

- **Simplicity** – for a non-technical/non-expert audience by using plain language and presented as checklists and bullet points wherever possible; this will also support easier translation from English to other languages.
- **Trainability** – to be easily transformed into training materials and building upon existing good practices already recognised and trained in the security and counter-terrorism sectors.

- **Transferability** – to be complementary and transferable to other deliverables across the project using commonly defined terminology; particularly in the case of the public awareness campaign (WP7). The procedures will be maintained as an open working copy to remain adaptable for that purpose.
- **Scalability** – to be applicable and usable primarily for large religious gatherings but also scalable and applicable to smaller ones wherever possible.

The set of procedures include the following:

- **GUIDE** for incident managers of terrorist/extremist threats and attacks - defines the role, responsibilities and procedures for the incident manager at the place of worship (essential for all types of emergency management) in the context of a terrorist/extremist threat or attack. This could be a Head of Security or other specially trained senior member of staff. In majority cases, it is necessary to consider that a rabbi, priest, imam or other religious leader would be the person 'in charge' of a large religious gathering (and in immediate control of the public address system) and may need to be trained in this role and procedure. The procedure also sets out the capabilities the incident manager will need to rely on in their role to successfully implement the procedure.
- **GUIDE** for interoperability with the emergency services - sets out a series of good practises so the place of worships receives (and supports) a fast and efficient response from the emergency services to a terrorist/extremist threat or attack through advanced joint planning, plans and exercising.
- **GUIDE** for developing a Welcome Team - sets out how a team can be formed to receive worshippers and visitors at large gatherings and events who are trained and exercised in security and emergency procedures to provide an increased and improved capability for the place of worship in detecting, deterring and delaying general security threats - including terrorist/extremist threats and attacks.
- **ADVICE** for the public to stay safe during a terrorist/extremist attack - sets out the public awareness campaign materials on this topic (WP7) and the set of procedures builds on these principles and complements them; it should be recognised they are not procedures to be implemented by the place of worship.
- **ADVICE** for the public to stay safe during a CBRN incident - sets out the public awareness campaign materials on this topic (WP7) and the set of procedures builds on these principles and complements them; it should be recognised they are not procedures to be implemented by the place of worship.
- **ACTIONS** to take IMMEDIATELY following a CBRN incident - sets out a procedure to recognise, assess and react to a CBRN threat/attack; including a quick, effective and low-cost method of immediate decontamination that could be managed by staff/security/welcome team if trained accordingly.
- **OPTIONS** for the emergency response to a terrorist/extremist threat or attack – sets out a summary of the various tactical options available to the incident manager/staff.

- **GUIDE** for evacuation planning – sets out how to implement a full, partial or zonal evacuation in response to a terrorist/extremist threat or fast-moving incident such as an explosive, firearms or weapons attack. The procedure should be applied and adapted to the particular design, layout and infrastructure of the place of worship or event. An evacuation plan could be developed from the procedure by adding maps/floorplans identifying all evacuation routes with supporting notes about each option. A section on communications is also included.
- **GUIDE** for invacuation planning – sets out how to implement a full, partial or zonal invacuation in response to a terrorist/extremist threat or fast-moving incident such as an explosive, firearms or weapons attack; including the identification/development of protected spaces. The procedure should be applied and adapted to the particular design, layout and infrastructure of the place of worship or event. An invacuation plan could be developed from the procedure by adding maps/floorplans identifying all invacuation routes with supporting notes about each option. A section on communications is also included.
- **GUIDE** for lockdown planning – sets out how to implement a full, partial or zonal lockdown in response to a terrorist/extremist threat or fast-moving incident such as an explosive, firearms or weapons attack. The procedure should be applied and adapted to the particular design, layout and infrastructure of the place of worship or event. A lockdown plan could be developed from the procedure by adding maps/floorplans identifying all invacuation routes, safe rooms and protected spaces with supporting notes about each option. A section on communications is also included.
- **ACTIONS** to take when a suspicious item of mail, package or substance is discovered - sets out how to react to these items in a format that can be used as a reminder to staff, to record the details and make an internal report. An illustration of suspicious characteristics can also be used as a training aid.
- **ACTIONS** to take if a bomb threat-hoax is received - sets out how to react to these items in a format that can be used as a reminder to staff, to record the details and make an internal report.
- **ACTIONS** to take when a suspicious item is discovered - sets out how to react to a potentially suspicious item reported or found; provides a checklist to decide if it should be treated as lost property or suspicious and what actions to take if it is considered suspicious.
- **CHECKING** your venue for suspicious items – sets out how to organise a reactionary or defensive search.

1. GUIDE for incident managers of terrorist/extremist threats and attacks

The incident manager has overall responsibility and authority for decisions and resources during an emergency. In the case of a terrorist/extremist threat or attack the aim of the incident manager is:

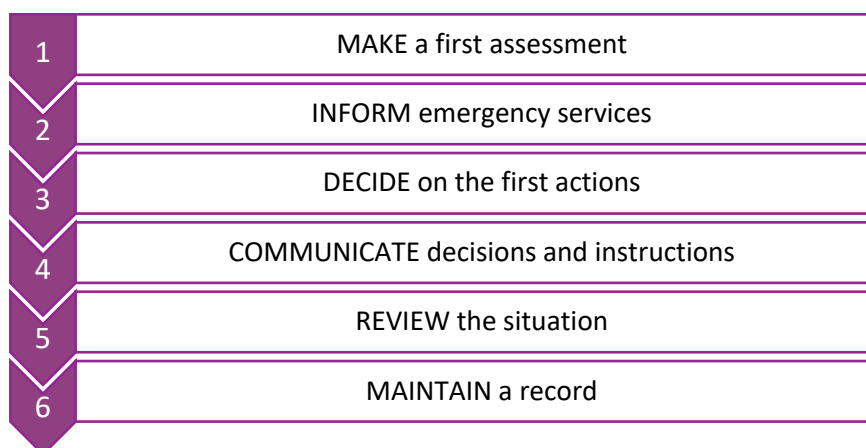
- Protecting people (and property) from harm by keeping them as safe as possible
- Deterring and delaying the threat/attack as much as possible
- Informing the emergency services with timely and accurate information while waiting for them to attend and deal with the threat/attack

In the case of most large-scale events and large gatherings, there should be an event plan that contains emergency procedures clearly defining roles, responsibilities and the actions to be taken in the case of various emergency situations. This should include the role and responsibilities of an incident manager in charge of the response on behalf of the place of worship. The incident manager should act in accordance with the plan. When the emergency services are involved and integrated into the event or large gathering, the incident manager for the place of worship will usually act on the guidance and instructions of the emergency services to support the overall response to the emergency situation by communicating and coordinating the response of the place of worship.

In the case of events and large gatherings without an emergency services' presence and without a specific event or emergency plan, there should always be a nominated incident manager in place to take responsibility and authority during an emergency situation. Put simply, somebody must have responsibility for leading and coordinate the response during an emergency situation; they should know they are the responsible person, and staff should also know who is responsible so they are ready to implement any decisions that are made. The incident manager will hand over the management of the threat/attack to the emergency services as soon as possible after their arrival; the incident manager for the place of worship will continue to act in a supporting role to the emergency services by coordinating the response of the place of worship.

In the case of a terrorist/extremist threat or attack the incident manager must conduct steps mentioned in Figure No 2:

Figure 2 – Steps made by incident manager



1.1. MAKE a first assessment:

- Consider if the threat/attack is credible and requires a response or not.
- Based on all the currently available information, recognising it may be incomplete.
- Establish as much as possible about:
 - What has happened? (it's nature, scale)
 - When did it happened? (Timeline, ongoing or not)
 - Where is the threat / incident / attack? (Location(s), weapons involved, static or moving/changing)
 - Who is involved? (Attacker(s), descriptions, direction of travel, casualty types/numbers/location(s))
 - Why has it happened? (motive/explanation, context)
- Initiate enquiries to fill any information gaps and then update/maintain situational awareness.
- Confirm if the emergency services have already been informed, if they provided any guidance or instructions and if they are attending.

1.2. INFORM emergency services

- It is critical to alert emergency services about a credible threat/attack immediately so they can mobilise their resources to attend. A nominated person should do it and report back when it is done. An uncertain situation can also be reported to the emergency service for their general information and to receive advice from them.
- Make the fullest possible first report (or updated/second/confirmatory report) as soon as possible. The ETHANE structured report (Figure No. 3) to provide the key information needed by the emergency services:

Figure 3 – ETHANE structure report



- ✓ **Exact location** - precisely where the threat/attack is, what part of the site/building(s) are affected, report where any attackers were last seen and where they were going
- ✓ **Type of incident** - what type of incident/threat/attack (suspicious package, bomb threat, active shooter, attack with a bladed weapon etc.)
- ✓ **Hazards** - what hazards/potential hazards are involved (possible explosives, weapons seen/used, CBRN materials etc.), report description(s) of the attacker(s)
- ✓ **Access** – what are the best routes for emergency access and exit (consider options from any plans previously agreed/held by emergency services)
- ✓ **Number of casualties** - how many and what type of injuries
- ✓ **Emergency services** – which ones and how many are there, which ones and how many are needed for the specific threat(s), hazard(s) and impacts of the emergency situation

Important highlight:

Assume that an updated/second/confirmatory report should be made after your first assessment so emergency services can be updated, confirm their expected attendance/time, and confirm/update any previous guidance or instructions that were given and provide any updated advice.

1.3. DECIDE on the first actions

- ✓ Recognise THEY must take personal responsibility to manage the response to a credible threat/attack until the emergency services attend and take over.
- ✓ Follow any guidance or instructions given by the emergency services.
- ✓ Decide to implement the best tactical option(s) to protect people (and property) to keep them as safe as possible while waiting for the emergency services to attend and deal with the threat/attack. This may involve a mixture of evacuation/invacuation/lockdown depending on the characteristics of the site and the assessment of the threat/attack.
- ✓ Implement measures (if possible) to deter and/or delay the attack while keeping people as safe as possible.
- ✓ Recognise that quick decisions may be needed about evacuation / invacuation / lockdown to keep people safe based on incomplete information about the threat/attack.
- ✓ Delaying decisions while waiting for more information may put people at increased risk from the threat/attack.

1.4. COMMUNICATE decisions and instructions

- ✓ To staff - about evacuation/invacuation/lockdown implementation using predetermined protocols/alarms/code words (but NOT fire alarm for evacuation). REMEMBER that attackers may hear any instructions given on PA system or Radios (such as location of protected spaces).
- ✓ To worshippers - use pre-scripted clear and concise messages to provide instructions about where to go and what to do. REMEMBER that an evacuation may need to be followed by a dispersal rather than an assembly.
- ✓ To neighbours - so they can take action to keep themselves and other safe in accordance with their own emergency plans and procedures.
- ✓ To emergency services - keep them regularly updated on developments and relevant new information while they are on their way, so they are prepared with the best understanding of the situation (keep updating the key information using ETHANE reports).
- ✓ By delegating clearly specified tasks and messages to nominated/trained staff such as communications with emergency services, neighbours, making the pre-scripted public announcements etc.

1.5. REVIEW the situation

- ✓ By actively monitoring and understanding the developing situation and the activities of staff who are implementing the emergency procedures.
- ✓ By making further/updated assessments based on any new/changing information.
- ✓ By sharing information with the emergency services (using updated ETHANE reports) and receiving any new/updated guidance or instructions from them.
- ✓ By developing and implementing the best possible actions/response(s) by confirming/adapting decisions and by making new ones based on the changing situation and advice of the emergency services.
- ✓ By clear, concise and timely communications with staff, worshippers and neighbours.

1.6. MAINTAIN a record

- ✓ Of information received and requested for building and maintaining the situation awareness (including timings, who requested/provided).
- ✓ Of decisions made (including timings) and the supporting reasons (what options were considered, the rationale for rejecting/accepting specific options).
- ✓ Of significant communications that were made (to who, including timings).

The incident manager will need to rely on the following capabilities as the basis for implementing an effective response to terrorist/extremist threats or attacks:

1.7. Personal Training

Personal training for their role and responsibilities, including opportunities to rehearse and exercise them.

A Plan

Setting out tactical options for responding to a terrorist/extremist threat or attack; with reference to the specific threat context and vulnerabilities of the place of worship/event.

A Location

A preferred secure location known to staff for carrying out incident management functions with sufficient security, access to communications, resources, CCTV, copies of plans and contact lists. Back-up options should also be identified in case the preferred location is compromised by the incident. The emergency services should also know where to find/consult the incident manager and take over responsibility for incident management from them as soon as possible after arriving at the scene.

Relevant emergency procedures

Designed specifically for the characteristics of the site/event.

Staff/Teams

The human capacity for implementing the tactical options and emergency procedures; they must be familiar with the plans/options/procedures and have been trained/exercised in them - particularly evacuation (including non-fire), invacuation and lockdown; this should include nominated staff/roles for leading and implementing specific procedures. Individuals from the religious or administrative staff and volunteers can be included. The role of the incident manager is a critical function, and they should always have a nominated deputy available to take over their role (maintained competency/training, updated call out lists etc.).

Communications

Tested and reliable communications capabilities for giving/ receiving/exchanging information/decisions with staff; to announce information and instructions to worshippers; contact lists for emergency situations (internal and external); nominated staff/teams for delegation of communications tasks.

2. GUIDE for interoperability with the emergency services

Advance consultation and joint planning/plans between the emergency services and the place of worship is good practice to ensure a timely and effective response by the emergency services and place of worship in case a terrorist/extremist threat or attack was to ever occur.

The best pre-determined options and locations for emergency activities should be selected, agreed and included in plans held by the emergency services and the place of worship (including the operator/managing body of the site), examples include:

- Forward command post(s) - for a representative from the place of worship to attend and provide cooperation, support and coordination of the response.
- Rendezvous Point(s) for emergency services - for their resources to assemble close to the scene and for briefings of their staff so they can be deployed.
- Triage and treatment areas - for emergency medical services to establish their medical responses for processing casualties and transport them to medical facilities for further treatment if necessary.
- Mass decontamination area(s) - for large scale decontamination of people if needed as a result of a CBRN incident/attack.
- Traffic Management plan(s) - to ensure speed of access to the site/event for emergency vehicles and implementation of road blocks/diversions to keep people and traffic safely away from the area, to deal with potential points of congestion that may impede their response and ensuring ambulances can leave the area to transport casualties to hospital.

The place of worship should:

- ✓ **Design** specific emergency procedures to complement and facilitate the emergency services' response plans into their own plans (such as closing car parks so people leaving in their vehicles will not block emergency service access and/or surrounding road networks).
- ✓ **Share** their emergency plans and procedures with the emergency services so evacuation/invacuation/lockdown plans and routes are known together with any designated protected/refuge areas where worshippers may be directed to shelter.
- ✓ **Plan** where and how they will hand-over incident management responsibility to the emergency services as soon as possible after they arrive at the scene and provide ongoing support to them by coordinating the response of the place of worship (consider access to CCTV, public and staff communications etc).
- ✓ **Agree** a procedure for reversing lockdown and the release of people from protected/refuge areas so emergency services have a predetermined and structured approach to this aspect of their intervention and the rescue of worshippers who are sheltering inside the place of worship (and staff at the place of worship can be trained accordingly).



Exercise their plans and procedures with the emergency services to test and validate them, which can also provide an opportunity for staff training and rehearsal and mutual learning that can lead to improvements to plans, procedures, cooperation and interoperability.

3. GUIDE for developing a Welcome Team

In keeping with the open and welcoming ethos and culture of places of worship, it is recommended that 'Welcome Teams' are formed to receive worshippers and visitors at large gatherings and events who are trained and exercised in security and emergency procedures to provide an increased and improved capability for the place of worship in detecting, deterring and delaying general security threats - including terrorist/extremist threats and attacks.

Welcome Teams can be developed at places of worship as a primary means of delivering some security capability where no formal security staff (or team) are deployed. A Welcome Team may also be developed to supplement and reinforce existing security staff/team capabilities. Some places of worship may be able to develop existing teams of non-security staff (and/or volunteers) based on the Welcome Team principles.

3.1. Role of the Welcoming Team

There are two primary roles which can be adapted according to the individual preferences and requirements of the place of worship:

- Welcoming worshippers and visitors and providing them with general information and support as needed/requested (such as handing out information leaflets about the event/future events, directions to parking/seating, answering questions about the venue and facilities).
- Monitoring, reporting and responding to potential security threats/risks (such as suspicious items or behaviour) and implementing emergency procedures, when necessary, in response to a potential or actual emergency (such as a credible threat from a suspicious/unattended item, a serious incident, a terrorist/extremist threat or attack).

3.2. Staff and/or Volunteers

- Selection and recruitment should be linked to the dual roles of hospitality and security (such as good interpersonal and communication skills combined with good observations skills, problem-solving and confident decision-making).
- Selection and recruitment could be made from the worshipping community with the added advantage of being recognised, known, trusted and familiarised with the site as well as being personally invested in the activities/ community of the place of worship.
- Selection and recruitment could be based on previous relevant skills and experience (such as in the hospitality sector or previous service in the military/emergency services).

3.3. Deployment

- The team should be clearly identifiable to worshippers and visitors by some means. This can be considered and decided by each place of worship according to their particular culture, customs and preferences and depending on how visible and noticeable they would like the team to be (such as a badge, a corporate item of clothing worn by them all, a uniform, a reflective jacket - perhaps marked as 'Welcomer' or something similar).
- The team should (ideally) be deployed at key points according to the findings of the vulnerability assessment and across all the specified phases of security – phase 1 access roads, phase 2 parking, phase 3 approach to venue, phase 4 arrival area, phase 5 access to venue (areas

without access control), phase 6 access to venue (areas with access control). This will provide a strong capability for early monitoring/recognition of a potential or actual threat/risk and for early counter measures/emergency procedures to be implemented across all the phases of site security.

- Welcomers should (ideally) be deployed in pairs. This will provide the best capability and opportunity for monitoring, assessing, responding and reporting potential or actual threats and for implementing any emergency procedures. Safe and effective systems of working could more easily be achieved in pairs (such as a staff member supported by a volunteer, one team member dealing with a suspicious item/behaviour item while the second reports it by radio, two team members to implement an emergency procedure more quickly).
- The presence of a recognisable team (ideally) across all the phases of security will deliver a visible security deterrent and provide reassurance about safety and security to worshippers and visitors.

3.4. Communications

- Consideration should be given to the variety of communications options that can be made available to the Welcome Team (such as personal radios, mobile phones, social media/chat groups, public announcement systems).
- Communications capacities and limitations should be fully tested and understood (such as what area(s) can/cannot hear a public announcement system broadcast, mobile phone signal viability in protected spaces). Communications capabilities should be regularly tested, exercised and maintained.
- Training in any code words used to invoke emergency procedures or indicate specific locations must be regularly conducted and reinforced to avoid any confusion if/when they are used.

3.5. Training

Welcome Team staff (and/or volunteers) will need to be trained in:

- Core skills (such as customer service, communication skills, problem solving and decision-making).
- Basic security awareness, particularly in the recognition, reporting and response to suspicious items and behaviour such as defensive searching of buildings, procedures for reporting incidents to the emergency services).
- Event/site plans at the place of worship to understand how events are organised and managed, how crowd movements can be managed and where critical services are resources are located.
- Implementing emergency procedures, particularly evacuation (fire and non-fire), invacuation (sheltering, hiding), CBRN (steps 123+, Remove x3) and lockdown (to include reinforcement and validation by using role play, rehearsals and exercises).

4. ADVICE for the public to stay safe during a terrorist/extremist attack



RUN

- Escape if you can
- Consider the safest options
- Is there a safe route? RUN, if not HIDE.
- Can you get there without exposing yourself to greater danger?
- Help other people to escape, but don't let their indecision slow you down
- Leave belongings behind
- Do not attempt to film the incident – run
- Alert people around you and deter them from entering danger zone



HIDE

- If you cannot run, HIDE
- Find cover from gunfire e.g., substantial brickwork / heavy reinforced walls
- If you can see the attacker, they may be able to see you. Cover from view does not mean you are safe. Bullets go through glass, brick, wood and metal.
- You must still hide, even if you are behind a locked door.
- Be aware of your exits
- Try not to get trapped
- Turn off light and mute the devices
- Be quiet, silence your phone and turn off vibrate
- Lock / barricade yourself in and move away from the door

**TELL**

If you cannot speak or make a noise, listen to the instructions given to you by the call taker:

- Call 112 - If you cannot speak or make a noise, listen to the instructions given to you by the call taker
- What do the police need to know?
 - Nature of the Incident – What is happening?
 - Location – where is the incident taking place? Give an address or general location
 - Suspects – Where are the suspects?
 - Direction – Where did you last see the suspects?
 - Descriptions – Describe the attacker, numbers, features, clothing, weapons etc.
 - Further information – Casualties, type of injury, building information, entrances, exits, hostages etc
- Follow police instructions
- Remain calm
- Avoid sudden movements that may be considered a threat
- Keep your hands open and in view

**POLICE MAY**

- Point guns at you
- Treat you firmly
- Question you
- Be unable to distinguish you from the attacker
- Officers will evacuate you when it is safe to do so

5. ADVICE for the public to stay safe during a CBRN incident

- REMOVE yourself from the area and get away from anything that may be dangerous like:
 - unusual smells
 - unexplained vapor or mist clouds
 - dead or unwell people or animals
 - oily droplets or films on surfaces or water
 - unusual materials or equipment
- Choose perpendicular way to the wind direction
- Even if you feel unwell, DON'T sit or lie down, you might not be able to get up again
- If inside, try to go outside into fresh air if possible
- If you see people who are unwell or passing out, help them leave the area without retracing your steps
- As soon as you get to a safer area, carefully REMOVE your outer clothing – it may be contaminated:
 - DON'T touch the outside surface of the clothing with your hands
 - DON'T let the outside surface make contact with your face when you take off clothing
 - IF POSSIBLE try to isolate clothing in a plastic bag – like a garbage bag - or leave them on the ground and keep away. Tell emergency responders where they are when they arrive to help
 - IF POSSIBLE, REMOVE any hazardous substance from your skin using a dry absorbent material to soak it up or brush it off. RINSE continually with water if the skin is itchy or painful
- Use your mobile phone to alert the emergency services on 112 about:
 - The location of the incident
 - Your location (if different)
 - That hazardous materials might be involved
- WAIT for emergency services and follow their instructions
- DON'T go home because you may contaminate your family
- DON'T visit a medical facility, you may contaminate other people and emergency workers
- The emergency services will organize a place nearby where you can receive medical treatment
- DON'T touch anyone
- DON'T touch your face
- DON'T drink, eat or smoke

6. ACTIONS to take IMMEDIATELY following a CBRN incident

These actions can significantly improve the outcome for everyone



RECOGNISE - THE INDICATORS OF A CBRN ATTACK

Any one of these may be indicators of a CBRN incident & multiple indicators may increase the likelihood that it is CBRN-related

Physical symptoms:

- Disorientation and sweating
- Twitching and convulsions
- Airway irritation and breathing difficulties
- Eye and skin irritation
- Nausea and vomiting

Signs – two or more people incapacitated for no explainable reason:

- Unexplained liquids, powders or vapours
- Unexplained smells or tastes
- Unusual and/ or unattended materials, devices or equipment
- Dead insects, animals or withered plants



ASSESS - THE INCIDENT TO INFORM AN APPROPRIATE RESPONSE STRATEGY

Stay safe - do not put yourself or others in danger to assess the incident

- Where are CBRN indicators present?
 - To avoid moving people on the site through affected routes.
- Where are **casualties** located?
 - To identify who is exposed and advise Emergency Services.
- Where are other people on the site located?
 - To identify who isn't exposed and nearby routes for evacuation.
- Which routes are unaffected?
 - To identify unaffected routes for evacuation of people on the site.

- Are there any obvious secondary threats?
 - To reduce the risk of a further non-CBR attack.

If there are significant external hazards consider moving people to a safer area upwind or inside if possible.



REACT - APPROPRIATELY TO REDUCE THE HARM TO EVERYONE

Communicate:

- With emergency services as soon as possible, and say what you see

REMOVE, REMOVE, REMOVE message to all those affected (Figure No. 4)

- With people on the site to move them to an unaffected location via unaffected routes

Act:

- To prevent **all but essential** access to **affected** locations
- To keep potentially exposed individuals in an unaffected location, separate from those unexposed
- On planned processes to modify **building functions** e.g., lifts and aircon systems if appropriate

Important:

Stay safe - do not put yourself or others in danger to assess the incident.

Figure 4 – Remove, Remove, Remove

TELL THOSE AFFECTED TO:



REMOVE THEMSELVES...
...from the immediate area to avoid further exposure to the substance. Fresh air is important.
If the skin is itchy or painful, find a water source.



REMOVE OUTER CLOTHING...
...if affected by the substance.
Try to avoid pulling clothing over the head if possible.
Do not smoke, eat or drink.
Do not pull off clothing stuck to skin.



REMOVE THE SUBSTANCE...
...from skin using a dry absorbent material to either soak it up or brush it off.
RINSE continually with water if the skin is itchy or painful.

Source: UK National Counter Terrorism Security Office, UK (2018) - <https://www.protectuk.police.uk/advice-and-guidance/response/remove-remove-remove-guidance-hazardous-substance-exposure>

7. OPTIONS for the emergency response to a terrorist/extremist threat or attack

All the options should be implemented in accordance with any national laws and respect any regional or local regulations or conditions which may be different among Member States.

7.1. No action required

When the threat is considered implausible and it is reasonable and proportionate, after evaluation not to evacuate or invacuate (such as a hoax). Police may provide additional advice and guidance about other risk management options. Staff familiar with the site could be asked to check their immediate surroundings to identify anything out of place, making them aware of what to look for and considering that a 'hoax' may have been a test of your response as part of a hostile reconnaissance operation.

7.2. Full Evacuation

When reasonable to assume the attack or threat is credible, and when evacuation will move people towards a place of greater safety. Direct everyone to 'evacuate to their nearest exit' and disperse or direct them to specific exits. In some cases, this may be requested/directed by police.

7.3. Partial / Phased / Zonal Evacuation

When priority is given to the people closest to, or most at risk from the threat who are evacuated before others. Reduces overloading of internal or external circulation routes when evacuating large numbers of people. Direct each group/zone to 'evacuate to their nearest exit' and disperse or direct them to specific exits.

7.4. Directional Evacuation

When a specific area is, or is likely to become dangerous, or an alternative route would cause people to pass through (or near) the area of threat. Direct people to 'evacuate to a SPECIFIED exit' and disperse. This may increase overall evacuation time but could improve safety

7.5. Invacuation

When it is safer to move people away from the threat while remaining inside the venue. If the threat is outside, or the location is unknown, it can be more dangerous to evacuate if the route takes them past, or closer, to the threat (such as a suspect device, contaminated environment or an ongoing external attack) and may expose them to greater danger (such as death or injuries from blast fragments and glass). Moving people inside the venue is often safer than evacuating them to the outside; especially if they can be directed to pre-identified safer/protected spaces. Direct people to move quickly to SPECIFIED PLACES and AVOID naming the specified places on any public address system in case attackers overhear the location(s). Rely on staff who have been trained and practised in the invacuation procedure to direct people and lead them to the safer/protected spaces.

7.6. Full Lockdown

When preventing an attack has not been possible, and the entry of the threat/attacker(s) could make those inside more vulnerable. The ability to frustrate and delay the attacker(s) and reduce the number of potential casualties may be greatly increased by a complete lockdown of the site; especially for keeping the threat/attacker(s) outside. This could lead to people being 'locked outside' and more vulnerable to the threat; each case must be assessed on the information known. Good internal and external information and communications systems will be necessary to quickly activate the implementation of the full lockdown by staff and inform people to 'stay inside' and to be ready to follow any further instructions of the staff (in anticipation that movement to a safer/protected space may follow).

7.7. Partial / Phased / Zonal Lockdown

When preventing an attack has not been possible, and the threat/attackers have (or are) entering and putting those inside at risk. The ability to frustrate and delay the attacker(s) and reduce the number of potential casualties may be greatly increased through a partial, phased or zonal lockdown of the site; especially during the entry phase of an attack. This may be a more localised and targeted lockdown closest to the threat; and/or closest to large groups that can be quickly protected; and or key points that can substantially delay and frustrate the progress of the attacker(s) (such as stairwells). This may be more easily and quickly achieved than a full lockdown. The purpose of delaying an attacker is to either make it more difficult for them to reach their target, thus protecting people and property, or to slow down their escape from a scene and raise the chance of their apprehension by the authorities. Staff can progressively and dynamically develop and extend the lockdown according to the nature of the threat/attack and their own capabilities to implement the measures. Good internal and external information and communications systems will be necessary to quickly activate the implementation of the partial/phased/zonal lockdown by staff. Inform people to 'stay inside' and to be prepared to follow any further instructions of the staff (in anticipation that movement to a safer/protected space may follow).

8. GUIDE for evacuation planning

Implementing a full, partial or zonal evacuation in response to a terrorist/extremist threat or fast-moving incident such as an explosive, firearms or weapons attack is very challenging and can only be effective if adequate planning, training and rehearsal have been undertaken.

The following principles should be applied and adapted to the particular design, layout and infrastructure of the place of worship or event:

- Recognise that an evacuation in response to a terrorist/extremist threat or attack will need to be different to a fire evacuation (DON'T use certain fire exits close to the threat/attack, disperse DON'T assemble, DON'T use fire alarm, a DIFFERENT emergency evacuation plan for staff/volunteers/worshippers with disabilities etc).
- Identify how the site can be zoned so partial/phased/zonal evacuations can be controlled and prioritised to minimise the overloading of internal or external circulation routes.
- Consider the suitability, capacities and limitations of exit routes (such as trip hazards, lighting, 'pinch-points' etc.) and ensure they are regularly reviewed.
- Consider using 'improvised' methods and points of exit during a terrorist/extremist attack (such as ground floor windows to a safe outside area if an attacker has entered the building).
- Consider that the safety of particular routes may change during the course of an attack. For example, the use of lifts (in non-fire scenarios) may reduce evacuation times, but send people to an area where attackers may be located.
- Different routes and the names of the exits should be clearly labelled and familiarised to staff.
- Evacuation procedures should also put adequate steps in place to ensure no one else can enter the area once an evacuation has been initiated.
- For CBRN incidents, consider evacuating uphill and upwind, staying away from the building heating and ventilation systems if the incident occurred inside the building.
- In an emergency evacuation during an attack, it is possible that staff and worshippers may be directly and unavoidably confronted by an attacker. As a very last resort when there is a life-threatening situation, an attempt could be made to disrupt/delay and/or incapacitate the attacker by:
 - Acting as aggressively as possible against them
 - Throwing items at them
 - Improvising weapons from anything available that can be used to counter, disarm, immobilise them (such as scissors, hot liquids) or to keep them away from your personal space if they have a sharp object (broom, pole).
 - Working together with others in a team effort to overwhelm and incapacitate them
- Procedures need to be flexible enough to cope with and complement lockdown, invacuation and movement to safer/protected spaces.
- Include staff/volunteer roles and responsibilities and train/rehearse staff in the procedures.

Communication:

- DO NOT activate the fire alarm to initiate an evacuation; this can initiate an inappropriate response that may expose people to danger.
- Public announcement systems, if available, may provide more flexibility to provide information and instructions appropriate to the situation and confirm to staff/volunteers/worshippers that the emergency is real and reduce a potential delay in response.
- Direct people towards a place of greater safety informing them to 'evacuate to their nearest exit' and then to disperse, or direct them to specific exits e.g. Blue exit on 1st floor.
- Pre-scripted messages can be developed. Consideration should also be given to different target audiences (such as children, wheelchair users etc.)
- Communication without alerting attackers is important, so the use of code words (on public announcement systems or radios) would need to be included in planning, training and exercising.
- Ensure adequate communications are in place, particularly within and between protected spaces to:
 - Check that staff/volunteers can be accounted for
 - Communicate with the emergency/security team(s)
 - Communicate the status of the incident to staff/volunteers
 - Control movement of staff within or out of the protected space
 - Declare when the incident is over and it is safe to leave protected spaces/reverse any lockdown
- Ensure that staff/volunteers know their roles and remain contactable throughout the incident and understand procedures for contacting the emergency services. If evacuated people (and staff) disperse, ensure an adequate procedure for contacting and accounting for all staff afterwards.

9. GUIDE for invacuation planning

Implementing a full, partial or zonal invacuation in response to a terrorist/extremist threat or fast-moving incident such as an explosive, firearms or weapons attack is very challenging and can only be effective if adequate planning, training and rehearsal have been undertaken.

The following principles should be applied and adapted to the particular design, layout and infrastructure of the place of worship or event:

- There are occasions when it may be safer to move people away from the threat while remaining inside.
- If the threat is outside your venue, or the location is unknown, people may be exposed to greater danger if the evacuation route takes them past the threat (such as a suspect device, contaminated environment or an ongoing external attack).
- Glass and other fragments from IEDs may kill or injure at a considerable distance, moving people inside (including to protected spaces) is often safer than evacuating them to an outside area or onto the streets.
- Identify any 'safe room(s)' which have been specifically designed and constructed for sheltering people from an attack within your building(s) and include them in your emergency plans. Ensure they are properly maintained and stocked with essential supplies and understand the maximum sheltering capacity (and time) they can provide.
- Develop 'protected spaces' within your building(s) to more securely protect people and include them in your emergency plans. 'Protected spaces' can be used in the absence of purpose built 'safe rooms' or to supplement their sheltering capacity according to the anticipated needs of the place of worship. Protected spaces should:
 - Be located in areas surrounded by full-height masonry walls, e.g. internal corridors, toilet areas or large rooms with doors opening inwards
 - Be located away from windows and external walls
 - Be located away from the area between the building's perimeter and the first line of supporting columns (known as the 'perimeter structural bay')
 - Be located away from stairwells or areas with access to lift shafts which open at ground level onto the street (because if compromised, blast could travel up them. However, if the stair and lift cores are entirely enclosed, they could make good protected spaces)
 - Avoid using the ground floor or first floor if possible. Basements and attic spaces may be unsuitable in the case of a CBRN threat or attack.
 - Provide one or more areas with enough space to contain the anticipated number of occupants
 - Provide sufficient air, toilet facilities, seating, drinking water, lighting and communications (because they may be necessary to accommodate people for an extended period of a few hours or more). The ability to shut down any mechanical ventilation systems may be necessary in the case of a CBRN threat or attack to prevent contamination of the protected area.
 - Be consulted with a structural engineer who has knowledge of explosive, CBRN and ballistic effects

- Consider staff training and exercising in techniques for improvising/strengthening a safer area (or hiding places) by making effective barricades, using door wedges, remaining silent, instructing phones are switched to silent/non-vibrate, turning out lights, covering windows etc.
- In an emergency evacuation during an attack, it is possible that staff and worshippers may be directly and unavoidably confronted by an attacker. As a very last resort when there is a life-threatening situation, an attempt could be made to disrupt/delay and/or incapacitate the attacker by:
 - Acting as aggressively as possible against them
 - Throwing items at them
 - Improvising weapons from anything available that can be used to counter, disarm or immobilise them (such as scissors, hot liquids, furniture)
 - Working together with others in a team effort to overwhelm and incapacitate them
- Procedures need to be flexible enough to cope with and complement lockdown, evacuation and movement to safer/protected spaces.
- Include staff/volunteer roles and responsibilities and train/rehearse staff in the procedures.

Communications:

- Any evacuation will need to be supported by a communication giving clear and concise instructions. When crafting communications, consider both the effectiveness on staff but also how this may be received (and acted upon) by attackers. The crafting of these messages requires considerable thought and practice in delivery.
- Pre-scripted messages can be developed. Consideration should also be given to different target audiences (such as children, wheelchair users etc.).
- Communications systems could include internal public announcement systems, handheld radios or other stand-alone systems. Do not rely on mobile phones as they may not receive a signal in a protected space (this should be carefully tested).
- Ensure that staff/volunteers know their roles and remain contactable during the incident and understand procedures for contacting the emergency services.
- Ensure adequate communications are in place, particularly within and between protected spaces to:
 - Check that staff/volunteers can be accounted for
 - Communicate with the emergency/security team(s)
 - Communicate the status of the incident to staff/volunteers
 - Control movement of staff within or out of the protected space
 - Declare when the incident is over and it is safe to leave protected spaces/reverse any lockdown
- A procedure and codeword may need to be used to announce it is safe to leave a protected space so a hostage or staff member cannot be forced under duress to entice and 'trick' people out of a protected space or to open the door so the attacker(s) can enter.

10. GUIDE for lockdown planning

Implementing a full, partial or zonal lockdown in response to a terrorist/extremist threat or fast-moving incident such as an explosive, firearms or weapons attack is very challenging and can only be effective if adequate planning, training and rehearsal have been undertaken.

The following principles should be applied and adapted to the particular design, layout and infrastructure of the place of worship or event:

- Identify all access and exit points within both the public and private areas of the site. Access points may be more than just doors and gates.
- Identify how to quickly and physically secure access/exit points. Consider both the design of the locking device at these points and whose role it would be to secure them eg. key or manually operated, automatically/remotely controlled etc.
- Identify how lockdown can be quickly reversed if needed (such as in the case of a fire, an attacker breaking in, or CBRN contamination).
- Identify how to disable lifts without returning them to the ground floor.
- Identify how to stop people leaving or entering the site, and how people can be directed away from danger.
- Identify how your site can be zoned to allow specific areas to be locked down.
- In an emergency lockdown during an attack, it is possible that staff and worshippers may be directly and unavoidably confronted by an attacker. As a very last resort when there is a life-threatening situation, an attempt could be made to disrupt/delay and/or incapacitate the attacker by:
 - Acting as aggressively as possible against them
 - Throwing items at them
 - Improvising weapons from anything available that can be used to counter, disarm or immobilise them (such as scissors, hot liquids, furniture)
 - Working together with others in a team effort to overwhelm and incapacitate them
- Processes need to be flexible enough to cope with and complement evacuation, invacuation and movement to protected spaces.
- Include staff/volunteer roles and responsibilities and train/rehearse staff in the procedures.

Communications:

- Any lockdown will need to be supported by a communication giving clear and concise instructions. When crafting communications, consider both the effectiveness on staff but also how this may be received (and acted upon) by attackers. The crafting of these messages requires considerable thought and practice in delivery.
- Pre-scripted messages can be developed. Consideration should also be given to different target audiences (such as children, wheelchair users etc.)

- Communications systems could include internal public announcement systems, handheld radios or other stand-alone systems. Do not rely on mobile phones as they may not receive a signal in a protected space (this should be carefully tested).
- Ensure that staff/volunteers know their roles and remain contactable during the incident and understand procedures for contacting the emergency services.
- Ensure adequate communications within and between protected spaces to:
 - Check that staff/volunteers can be accounted for
 - Communicate with the emergency/security team(s)
 - Communicate the status of the incident to staff/volunteers
 - Control movement of staff within or out of the protected space
 - Declare when the incident is over and it is safe to leave protected spaces/reverse any lockdown
- A procedure and codeword may need to be used to announce it is safe to end the lockdown or leave a protected space so a hostage or staff member cannot be forced under duress to entice and 'trick' people to open a door so the attacker(s) can enter or to leave the protected space.

11. ACTIONS to take when a suspicious item of mail, package, substance is discovered

- LEAVE IT WHERE IT WAS FOUND - DO NOT TOUCH OR DISTURB IT - DO NOT CLEAN UP ANY SUBSTANCE
- CLEAR THE IMMEDIATE AREA of all people and keep others away
- INSTRUCT PEOPLE in the immediate area to WASH HANDS AND ANY EXPOSED SKIN with soap and water and tell them to wait for further instructions
- SHUT DOWN ALL EQUIPMENT in the immediate area used for heating, ventilation and air conditioning (HVACs)
- CORDON OFF THE IMMEDIATE AREA to keep people out and DIRECT PEOPLE AWAY FROM THE HAZARD
- RECORD IMPORTANT INFORMATION about the package, substance or mail item
- DO NOT USE MOBILE PHONES OR RADIOS in the cleared area or within fifteen metres of the package

EXACT LOCATION of suspicious package, substance or item of mail:

.....
.....
.....

DESCRIPTION of suspicious package, substance or item of mail:

.....
.....
.....

RECORD of any markings, labels or declarations on the suspicious package or item of mail:

.....
.....
.....

ADDRESSEE name and address:

.....
.....
.....

SENDER name and address:

.....
.....
.....

NAMES of people in the immediate area when found:

.....
.....
.....

- ✓ IF NOT AN IMMEDIATE EMERGENCY SITUATION - REPORT to INSERT INTERNAL PERSON/ROLE
- ✓ IN THE CASE OF AN EMERGENCY SITUATION - CALL THE EMERGENCY SERVICES 112

Figure 5 – Suspicious letter and package¹



¹ <https://uwaterloo.ca/central-stores/mail-pickup-delivery/suspicious-mail>

12. ACTIONS to take if a bomb threat-hoax is received

- ✓ REMAIN CALM AND TALK TO THE CALLER:
 - **DO NOT** put them on hold or cut them off
 - **ALERT SOMEONE** as quickly as possible
 - **OBTAIN** as much information as you can
 - **KEEP THE CALLER TALKING** (apologise for bad line, ask the caller to speak up, etc.)
 - **COMPLETE THIS FORM** during the call by asking the questions in sequence if necessary
 - **KEEP TELEPHONE LINE OPEN** even after the caller has disengaged as it might be traceable with technology
- ✓ RECORD THE CALL IF YOU CAN
- ✓ NOTE THE CALLER'S NUMBER IF DISPLAYED ON YOUR PHONE:
(for cases of social media or e-mail threat see below)
- ✓ WRITE THE EXACT WORDING OF THE THREAT:
 - When?
 - Where?
 - What?
 - How?
 - Who?
 - Why?
 - Time?

Notes...

- ✓ ASK THE FOLLOWING QUESTIONS AND RECORD THE ANSWERS AS ACURATELY AS POSSIBLE:

1. Where exactly is the bomb right now?

.....
.....

2. When is it going to explode?

.....
.....

3. What does it look like?

.....
.....

4. What does the bomb contain?

.....
.....

5. How will it be detonated?

.....
.....

6. Did you place the bomb? If not you, who did?

.....
.....

7. What is your name?

.....
.....

8. What is your address?

.....
.....

9. What is your telephone number?

.....
.....

10. Do you represent a group or are you acting alone?

.....
.....

11. Why have you placed the bomb?

.....
.....



IN CASES OF SOCIAL MEDIA OR E-MAIL BOMB THREATS:

- **DO NOT** reply to, forward or delete the message
- If sent via email note the address
- If sent via social media what application has been used and note the username/ID
- Preserve all web log files for your organisations to help the police investigation (as a guide, 7 days prior to the threat message and 48 hours after)



IMMEDIATELY INFORM THE BUIDING / SECURITY MANAGER SO THEY CAN REPORT THE BOMB THREAT TO THE POLICE AND DECIDE WHAT OTHER ACTION TO TAKE:

- Name of person informed:

.....
.....

- Time informed:

.....
.....

NOTES TO BE COMPLETED BY THE CALL-TAKER AS SOON AS POSSIBLE AFTER REPORTING THE BOMB THREAT

THE CALLER

Male	Female	Unsure	Age	Nationality

CALLER'S VOICE

Calm	Angry	Crying	Slow	Accent

Stutter	Lisp	Slurred	Disguised	If familiar, who did it sound like?

Deep	Laughter	Hoarse	Nasal

THREAT LANGUAGE

Aggressive	Taped	Incoherent	Irrational

BACKGROUND NOISE (DESCRIBE)

Street	House	Animal	Music	Other

Clear	Voice(s) machine PA system	Other noise, describe

Children	Aircraft

ANYTHING ELSE – UNUSUAL

ANYTHING ELSE – SIGNIFICANT

--	--

CALL DETAILS

Date of call		Time of call	
Time call ended		Phone number / extension of receiving	
Location where call was received		Details of any other witnesses to the call	

13. ACTIONS to take when a suspicious item is discovered



CONFIRM: if it has recognisable suspicious characteristics **USE 'HOT' ASSESSMENT**

IS IT HIDDEN?	Yes / No
IS IT OBVIOUSLY SUSPICIOUS?	Yes / No
Has the item been deliberately concealed or is it obviously hidden from view?	Yes / No
Does it have wires, circuit boards, batteries, tape, liquids or putty-like substances visible?	Yes / No
Do you think the item poses an immediate threat to life?	Yes / No
IS IT TYPICAL? ...of what you would expect to find in this location	Yes / No

Most lost property is found where people congregate, ask if anyone has left the item.

If the item is assessed to be unattended rather than suspicious, examine it further before using the lost property procedure BUT if the 'HOT' assessment leads you to believe the item is suspicious you should...



CLEAR: THE IMMEDIATE AREA

- Do not touch it
- Take charge and move people away to a safe distance. Even for a small item such as a briefcase move at least 100m away from the item starting from the centre and moving out (emergency may recommend at least 200m distance for a car sized explosive threat and 400m for a truck sized explosive threat).
- Keep yourself and other people out of line of sight of the item. It is a broad rule, but generally if you cannot see the item then you are better protected from it
- Think about what you can hide behind. Pick something substantial and keep away from glass such as windows and skylights
- Cordon off the area

**COMMUNICATE: CALL THE EMERGENCY SERVICES**

- Inform (INSERT NAME/INTERNAL ROLE OF PERSON IN CHARGE)
- Do not use mobile phones or radios within fifteen metres of the suspicious item

**CONTROL: ACCESS TO CORDONED AREA**

- The public should not be able to approach the area until it is considered safe
- Try and keep eyewitnesses nearby so they can tell the emergency services what they saw try to get contact details before witnesses move away

14. CHECKING your venue for suspicious items

Search Considerations

Regular searches of your place of worship will enhance a good security culture and reduce the risk of a suspicious item being placed or remaining unnoticed for long periods. Additionally, if you receive a threat and depending upon how credible it is, you may decide to conduct a 'search' for suspicious items. In such cases:

- ✓ **Ensure plans are in place** to carry out an effective search in response to a threat
- ✓ **Identify who in your venue** will coordinate and take responsibility for conducting searches
- ✓ **Initiate a search** by messaging over a public address system (using a coded messages avoids unnecessary disruption and alarm), by text message, personal radio or by a telephone cascade
- ✓ **Divide your venue** into areas of a manageable size for 1 or 2 searchers. Ideally staff should follow a search plan and search in pairs to ensure nothing is missed
- ✓ **Ensure those conducting** searches are familiar with their areas of responsibility. Those who regularly work in an area are best placed to spot unusual or suspicious items
- ✓ **Focus on areas that are open to the public**; enclosed areas (e.g. cloakrooms, stairs, corridors, lifts etc.) evacuation routes and assembly points, car parks, other external areas such as loading bays
- ✓ **Develop appropriate techniques for staff** to be able to routinely search public areas without alarming any visitors present. If more specialised techniques are considered (such as bag searches on entry) then specialised training, equipment and policies may be needed (such as what items should not be allowed inside the place of worship).
- ✓ **Ensure all visitors know** who to report a suspicious item to and have the confidence to report any suspicious behaviour.

Important:

Do not touch or move anything assessed as a suspicious item
– immediately start evacuation and dial 112.

Conclusions

This document provides a set of fourteen procedures to prevent, protect, detect, respond and mitigate the consequences of terrorist/extremist attacks at places of worship and large religious gatherings and protect the relevant stakeholders during an emergency situation. The procedures have been designed and developed with the principles of simplicity, trainability, transferability and scalability in mind so they can be implemented by staff at a large religious gathering or place of worship who may not be trained 'security professionals' but may have responsibility for managing the emergency response to an incident, threat or attack; including religious leaders that may be leading/officiating at the place of worship or event.

All the procedures should be considered in the context of national laws and respect any regional or local regulations or conditions which may be different among Member States and also take into account the capabilities and guidance from relevant public services, especially law enforcement agencies.

The effective implementation of the procedures will be highly dependent on the following factors:

- Adequate training for staff
- Awareness among worshippers
- Regular drills, rehearsals and exercises involving the procedures
- Cooperation with public services and key stakeholders
- Joint planning and interoperability with law enforcement agencies

The ProSPeReS project will provide relevant support for implementing the set of procedures by providing:

- A Manual for Vulnerability Assessment (Deliverable 2.1)
- A Guidebook, including recommendations of procedures, equipment and templates to prevent, protect, detect, respond and mitigate the result of the terrorist attack (Deliverable 3.3)
- A Security by Design Guidebook for Religious Sites (Deliverable 3.2)
- An Introduction to CBRN Threats, including security measures, scenarios and response option recommendations (Deliverables 4.1 & 4.2)
- A Training Curriculum, including trainer and trainee booklets and a virtual reality training platform (Deliverables 5.1-4)
- A Security Awareness Training Programme, including brochures, leaflets, videos and on-line materials (Deliverable 7.1-4)



prosperes.eu



This project is funded by the European Union's
Internal Security Fund – Police under Grant
Agreement No. 101034230 – ProSPeReS



Recommendations for equipment monitoring / detection / protection

Appendix 2

of GUIDEBOOK on security measures
for religious sites & communities

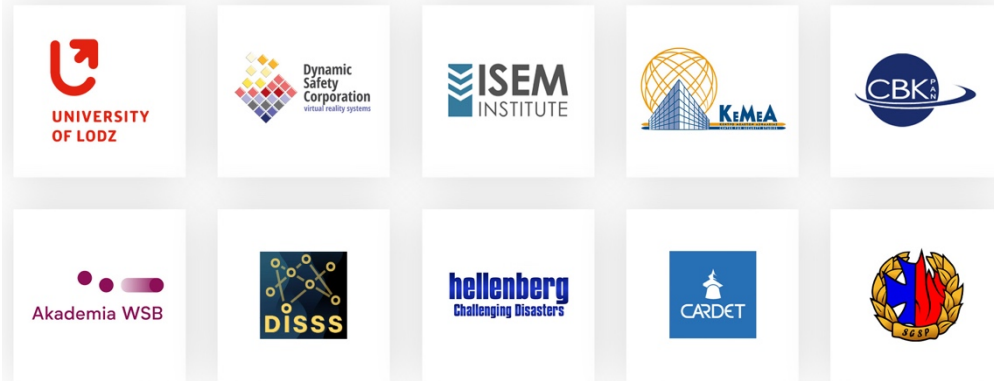


This project is funded by the European Union's
Internal Security Fund – Police under Grant
Agreement No. 101034230 – ProSPeReS

prosperes.eu

ProSPeReS consortium

Security experts, security research and academic institutions, providers of technical solutions and services



Law enforcement agencies (LEAs)



Faith-based organizations



Recommendations for equipment monitoring / detection / protection

Appendix 2
of GUIDEBOOK on security measures
for religious sites & communities

Document description

WP number and title	WP3 – Preparing the tailor-made security measures for religious sites. A3.4 – Preparing recommendations for equipment – monitoring, detection, and protection
Lead Beneficiary/Author(s)	UL (Dominik Klimas, Zbigniew Gajda)
Contributor(s)/Author(s)	UL, DSC, ISEMI, WSB, DISSS, HELLENBERG, CARDET, Archdioce. Lodz, Social Obser., HMI, GWZ Warsaw, KWP Lodz, KSP, KWP Wroclaw, HELLENIC POLICE, CBK PAN, SGSP
Document type	Report
Last Update	08/03/2023
Dissemination level	Public / Confidential *

* Confidential – only for members of the consortium & EC Services

Acknowledgement:

This project is funded by the European Union's Internal Security Fund — Police. Grant Agreement No. 101034230 — ProSPeReS

Disclaimer:

The content of this document 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.



This work is licensed under the Creative Commons Attribution 4.0 International Licence. To view a copy of this license, visit creativecommons.org/licenses/by/4.0/ with relevant national copyright provisions to be applied accordingly.

NOTE: Third party images have been used in this work in accordance with applicable fair use provisions for educational and demonstration purposes only. Relevant copyright or other rights apply accordingly. References to third party products are not commercial endorsements.

The material for this publication was developed and reviewed by ProSPeReS consortium:

No	Partner organization name	Short Name	Country
1	UNIVERSITY OF LODZ	UL	PL
2	DYNAMIC SAFETY CORPORATION	DSC	PL
3	INTERNATIONAL SECURITY AND EMERGENCY MANAGEMENT INSTITUTE	ISEMI	SK
4	CENTER FOR SECURITY STUDIES	KEMEA	GR
5	WSB ACADEMY	WSB	PL
6	STICHTING DUTCH INSTITUTE FOR SAFE AND SECURE SPACE	DISSS	NL
7	HELLENBERG INTERNATIONAL	HELLENBERG	FI
8	CENTRE FOR THE ADVANCEMENT OF RESEARCH & DEVELOPMENT IN EDUCATIONAL TECHNOLOGY LIMITED	CARDET	CY
9	ARCHDIOCESE OF LODZ	Archdiocese Lodz	PL
10	SOCIAL OBSERVATORY FOUNDATION	Social Obser.	PL
11	HOLY METROPOLIS OF IOANNINA	HMI	GR
12	JEWISH COMMUNITY OF WARSAW	GWZ Warsaw	PL
13	LODZ VOIVODESHIP POLICE	KWP Lodz	PL
14	WARSAW METROPOLITAN POLICE	KSP	PL
15	WROCLAW VOIVODESHIP POLICE	KWP Wroclaw	PL
16	HELLENIC POLICE	HP	GR
17	SPACE RESEARCH CENTRE POLISH ACADEMY OF SCIENCE	CBK PAN	PL
18	THE MAIN SCHOOL OF FIRE SERVICE	SGSP	PL

Table of Contents

List of Tables.....	8
1. Introduction to equipment recommendation.....	13
2. Types and level of threat.....	14
3. Equipment recommendation matrix	16
4. Facility security measures	22
4.1. Area 1 – External premises of the facility	22
4.1.1. Anti-intrusion barriers.....	22
4.1.2. Landscaping	23
4.1.3. Anti-ramming barriers	23
4.1.4. Security post.....	27
4.1.5. CCTV system	27
4.1.6. Waste containers.....	30
4.1.7. Drones solutions.....	30
4.2. Area 2 - Facility entry points	35
4.2.1. Entry/exit.....	35
4.2.2. Screening and detection equipment.....	37
4.2.3. Unauthorized opening door and windows alarm system	44
4.2.4. Interlocking door systems.....	45
4.2.5. Signage	45
4.2.6. Facade.....	46
4.2.7. Doors, glazing, and windows.....	46
4.3. Area 3 - Internal zone	50
4.3.1. Safe room.....	50
4.3.2. Mailroom.....	50
4.3.3. Control room.....	51
4.3.4. Public address/voice alarm system	52
4.3.5. Panic button.....	52

4.3.6. Integration systems - Physical Security Information Management (PSIM).....	53
4.3.7. Integrated Mass Notification System	54
4.3.8. Critical utility infrastructure	55
5. First response equipment	57
5.1. PPE.....	57
5.1.1. CBRN PPE	57
5.1.2. C-IED/Armed attack PPEC-IED/Armed attack PPE	69
6. Conclusions.....	78
List of References	79
Appendix A.....	80

List of Tables

Table 1. Risk Matrix Levels	15
Table 2. Equipment recommendation table	16
Table 3. Equipment recommendation table	16
Table 4. Equipment recommendation table	17
Table 5. Equipment recommendation	17

List of Pictures

Picture 1 – Wall spikes WSF-02	22
Picture 2 & 2a – RFID perimeter protection system.....	23
Picture 3 & 3a & 3b – SP 40, M50–1000 DFES bollards	24
Picture 4 – Roadblocker M50.....	24
Picture 5 & 5a – Bollards Furniture Urban	25
Picture 6 & 6a – F11, F18 mobile roadblock.....	25
Picture 7 – Mobile Road Blocker.....	26
Picture 8 – The Delta Cantilever Sliding Gate	26
Picture 9 – Colored Security Post.....	27
Picture 10 & 10a – CCTV system	28
Picture 11 – Screen capture from the Skylark system	28
Picture 12 – Abandoned Luggage Detection	29
Picture 13 – Body worn cameras	29
Picture 14 – DJI Mavic 2 Enterprise Advanced, DJI Matrice 300 RTK drones	30
Picture 15 – Drone recognition system screen capture from the Skylark system.....	31
Picture 16 – Drones accessories	31
Picture 17 – Antidrone net muncher Sky Wall 100	32
Picture 18 – Drone Catcher - Delft Dynamics BV	33
Picture 19 & 19a & 19b & 19c – Anti-drone system SkyCtrl	33
Picture 20 – Drone interceptor gun DroneGun Tactical	34
Picture 21 & 21a – Access Control Systems	35
Picture 22 – Turnstile gate REXON ERA 3.....	36
Picture 23 – Tripod twister Bar BA.....	36
Picture 24 – Handheld metal detector Super Scanner®V.....	37
Picture 25 – Garret Walk-thru metal detector	37

Picture 26 – X-ray scanner	38
Picture 27 – Handheld X-ray scanner NIGHTHAWK	38
Picture 28 – ENTRYSCAN® 4 - high-sensitivity high explosives walk-through detection system	39
Picture 29 – Smiths Detection SABRE 5000 chemical trace detector	39
Picture 30 – IONSCAN™ 500DT - simultaneous explosives and narcotics trace detector.....	40
Picture 31 – Ultra™ Multi-Target Explosives & Precursors Test Kit	40
Picture 32 – Gemini™ Combining Raman and FTIR technology Chemical Analyzer	41
Picture 33 – RAID-M100 Plus - Ion Mobility Spectrometry (IMS) hand-held Chemical Agent detector.....	41
Picture 34 – Drager Detection Tubes.....	42
Picture 35 – BioCheck™ Powder Screening Test Kit	42
Picture 36 – Qubit™ 3 Fluorometer	43
Picture 37 – NeutronRAE-II - personal radiation detector.....	43
Picture 38 – X-Ray and Gamma Personal Dosimeters PM1610A.....	44
Picture 39 – Open/Close Alarm Sensor for SCW Shield - 74WOS.....	44
Picture 40 – Man Trap Doors - Standard Telephones and Cables	45
Picture 41 – Surveillance Cameras In Use Signe	46
Picture 42 & 42a – Burglar resistance door and lock.....	47
Picture 43 – Blast Resistant Windows	48
Picture 44 – Safety and Security Window Films	48
Picture 45 – Anti-burglary window	49
Picture 46 – Mailsafe Bomb Box.....	51
Picture 47 – Public Address, Bosch Security and Safety Systems.....	52
Picture 48 & 48a – Panic button	53
Picture 49 – Physical Security Information Management system - GEMOS MOBILE	53

Picture 50 – Genasys Integrated Mass Notification System	54
Picture 51 & 51a – Dräger X-pect® 8100 Cover Spectacles, Dräger X-pect ® 8500 protective goggles	59
Picture 52 – Dräger X-plore® 1900 dust mask	60
Picture 53 – MSA Comfo Classic® Half-Mask Respirator	60
Picture 54 – Dräger CDR 4500 full-face mask	61
Picture 55 – G1 SCBA Self-contained breathing apparatus	61
Picture 56 & 56a – Dräger PARAT® 4700 escape hoods	62
Picture 57 – Dräger Saver PP Emergency Escape Breathing Apparatus.....	63
Picture 58 & 58a – Dräger Oxy K 30 H escape devices	63
Picture 59 – Safety gloves table	64
Picture 60 – Protective clothing table.....	65
Picture 61 – Protective suit 3M 4570	65
Picture 62 – CBRN response stages	66
Picture 63 & 63a – Decontamination process	67
Picture 64 – Decontamination equipment	67
Picture 65 – RSDL® Reactive Skin Decontamination Lotion Kit.....	68
Picture 66 – Skin decontamination by RSDL sponge	69
Picture 67 – Hercules Covert Stab, Spike and Needle Resistant Vest	70
Picture 68 – Ace Link Armor MSOV Modular.....	71
Picture 69 – DFNDR Armor Lightweight Level III+ armour plate	71
Picture 70 & 70a – Ballistic blanket.....	72
Picture 71 & 71a – Galvion helmet VIPER P4	72
Picture 72 & 72a – QS24 - Nomex® Comfort – Dupont Flame-resistance clothing..	73
Picture 73 – C-A-T® GEN7 - CAT Resources combat application tourniquet	74
Picture 74 – Burn dressing Water-Jel Technologies	74
Picture 75 – Hemostatic dressing CELOX RAPID	75

Picture 76 – Inspection cameras RIDGID CA-350X	76
Picture 77 – TSS Under Vehicle Search Mirror, Range: 4 Inspection mirror	76
Picture 78 & 78a – Hook and line kit.....	77

1. Introduction to equipment recommendation

Protecting religious facilities, their staff, and the worshippers is a great challenge. It must combine all the elements necessary for its proper functioning and not be an inconvenience to the congregants visiting the temple.

A proper and comprehensive approach to the subject often represents a substantial financial investment. This study is a guideline for solutions used in public buildings as a suggestion for existing applications. Not all of these solutions can be applied to every place, but they can be a guideline in which the equipment applications should be directed.

Malfunctions or improper preparation of the building security can expose the facility to many different hazards and risks, ranging from theft to the worst-case scenario of a successful terrorist attack. A poorly designed access control system makes it much easier to launch.

One of the critical goals of the multi-level protection concept is a comprehensive implementation of security measures integrating physical, technological, and operational standards.

From the technical point of view, a crucial point should be covered to ensure the safety of congregates arriving at the worship places.

The facility should be divided into a few areas of interest to approach this problem comprehensively.

The adaptation of technical protection systems should be tailored individually to the specific facility's needs, preceded by a specialized security audit.

The first source of information regarding enhancing security at a facility should be the local Law Enforcement Agencies (LEAs) responsible for conducting operations in the particular area in which the facility is located. Cooperation with the police is particularly important with regard to updating the threat level, cooperation on a daily basis and during the preparation as well as protection of an ongoing event, expert advice on procedures, and especially equipment recommendations. Due to its broad, specialized expertise in countering terrorist threats, it is a source of valuable information and support during the organization of events that gather large numbers of people.

2. Types and level of threat

Recommendations are a guide to identifying solutions that should be used to eliminate gaps in a facility's security system for a given type and threat level. These are divided into those for the facility, including its infrastructure and personnel. Any effort to equip the facility and personnel with appropriate technical measures should be preceded by a professional assessment of the facility's security safety measures and expert advice in adapting it to the current level and type of threats.

For the purposes of equipment recommendations, due to the complexity of the problem, they have been divided into 3 types of threats:

1. General terrorist acts (GENERAL).

This group includes other terrorist attacks unrelated to the IED and CBRN types of threats. These include but are not limited to:

- Sharp object attack,
- Firearms attack,
- Hand grenades/projectiles attack,
- Vehicle attack,
- Incendiary,
- Hostage-taking,
- Kidnapping.

2. Improvised explosive device (IED).

IED threats include one or more incidents involving improvised explosive devices, such as:

- IED detonation,
- Explosion,
- Find,
- Hoax,
- False,
- Turned-In.

3. CBRN.

Incidents include all threats involving the use of CBR agents regardless of whether they were triggered intentionally or unintentionally.

Intentional - CBRN incidents that involve the intentional release by states, non-state armed groups, terrorists, or criminals, with the intent to cause injury and death, cause fear and panic in individuals or a specific group of the local population.

Non-intentional - events related to industrial accidents, accidents in military research centers, related to accidents during the transportation of hazardous goods, natural sources of infection with bacteria or viruses, natural disasters leading to the destruction of industrial or military installations, and remnants of war.

However, this does not mean that every terrorist attack uses only one type of threat. Current trends indicate that terrorists are aiming for complex attacks, using each of the available weapons (firearms, bladed weapons, hand grenades, IEDs to CBR agents). Therefore, in the comprehensive preparation of a facility for terrorist attacks, all types of threats should be considered and implemented in security plans, technical upgrades, and individual equipment.

For the purposes of equipment recommendations for PW, the risk level for a given threat is determined based on the VAT light (Vulnerability Assessment Tool light), resulting from the assessed probabilities and consequences of threats.

Table 1 – Risk Matrix Levels

		PROBABILITY / LIKELIHOOD				
		Very Low (Insignificant)	Low (Minor)	Medium (Moderate)	High (Major)	Very High (Extensive)
CONSEQUENCES	Very Low (Insignificant)	Very Low	Very Low	Low	Medium	Medium
	Low (Minor)	Very Low	Low	Medium	Medium	High
	Medium (Moderate)	Low	Medium	Medium	High	High
	High (Major)	Medium	Medium	High	High	Very High
	Very High (Extensive)	Medium	High	High	Very High	Very High

Very Low/Low: is not considered a vulnerability. e.g., the attack can be mitigated by existing security measures.

Medium: is considered a vulnerability. e.g., the attack cannot be mitigated by existing security measures and should be mitigated by the managing body and its partners.

High/Very High: is considered a critical vulnerability. e.g., the risk cannot be mitigated by measures that the municipality and its partners can manage themselves.

3. Equipment recommendation matrix

The table is a pre-set tool designed to indicate minimum equipment recommendations based on the identified type of threat and its level. There is a specific equipment recommendation at the intersection of the identified threat level, the given area and the type of threat.

Suppose the threat for a given area is identified at the VERY LOW/LOW level. In that case, the recommendation also applies to the MEDIUM and HIGH/VERY HIGH levels (and on a similar basis, if a MEDIUM level is identified, it also applies to the HIGH/VERY HIGH threat level recommendation), as shown in the table below. On the right side of the table is a box with links to a brief description of existing solutions for the type and level of threat from different project resources.

Table 2 – Equipment recommendation table

			Threat	RISK LEVEL			Link to description
			GENERAL/IED/CBR	VERY LOW <u>LOW</u>	MEDIUM	HIGH VERY HIGH	
Object							
Structure	Fencing	GENERAL /IED/CBR	X	X	X	LINK	
	Land scaping	GENERAL /IED/CBR		X	X	LINK	
	Reinforced landscape objects	GENERAL /IED/CBR			X	LINK	
	Blast protection	IED			X	LINK	
	Blast door protection	IED			X	LINK	
	Ballistic door protection	GENERAL			X	LINK	

For example: Based on the VAT tool, a security analysis determined the threat level for a given facility as the MEDIUM for the IED threat.

Table 3 – Equipment recommendation table

			Threat	RISK LEVEL			Link to description
			GENERAL/IED/CBR	VERY LOW <u>LOW</u>	<u>MEDIUM</u>	HIGH VERY HIGH	
Object							
Structure	Fencing	GENERAL /IED/CBR	X	X	X	LINK	
	Land scaping	GENERAL /IED/CBR		X	X	LINK	
	Reinforced landscape objects	GENERAL /IED/CBR			X	LINK	
	Blast protection	IED			X	LINK	
	Blast door protection	IED			X	LINK	
	Ballistic door protection	GENERAL			X	LINK	
	Blast window protection	IED			X	LINK	
	Anti-fragmentation window films	IED	X	X	X	LINK	

According to the matrix, the person responsible for the facility's security checks the minimum recommended requirements that should be met to ensure an adequate security level. If there is an "X" mark in a particular area, it means that the solution is recommended for use.

After identifying a recommended security measure (e.g., anti-fragmentation window film), the person responsible for the security of a given facility moves to the "Link to description" tab leading to a description of existing solutions by clicking on the link.

Table 4 – Equipment recommendation table


Blast window protection			X	Link
Anti-fragmentation window films	X	X	X	Link

Table 5 – Equipment recommendation

Antifragmentation window film.

The substitute of the detonation blast resistant windows is the use of a protective film installed on the window glass. This solution can reduce the danger from an explosion by keeping glass shards together. Furthermore, the mechanical attachment of the film to the window frame further reduces the risk of the glass being pulled out of the frame during an explosion.

An added benefit is protection from thrown objects. It effectively stops even heavy, low-speed objects from falling into the object and protects against glass fragments. This solution is inexpensive, effective against thrown objects and to some extent reduces the effects of detonation of the explosive charge.



Safety and Security Window Films

In this way, he can identify whether the recommended solutions are installed at a given facility and, if so, whether they meet the relevant requirements for a given threat. The tool also indicates in which areas to seek specialized advice for technical modernization/equipment of the facility to improve its safety.

Any interference with a facility's security systems should be preceded by expert advice.

			Threat	RISK LEVEL			Link to description
			GENERAL/IED/CBR	VERY LOW/LOW	MEDIUM	HIGH/VERY HIGH	
Object							
Structure	Fencing	GENERAL /IED/CBR	X	X	X	LINK	
	Land scaping	GENERAL /IED/CBR		X	X	LINK	
	Reinforced landscape objects	GENERAL /IED/CBR			X	LINK	
	Blast protection	IED			X	LINK	
	Blast door protection	IED			X	LINK	
	Ballistic door protection	GENERAL			X	LINK	
	Blast window protection	IED			X	LINK	
	Anti-fragmentation window films	IED	X	X	X	LINK	
	Safe room	GENERAL /IED/CBR			X	LINK	
	Safe shelter	GENERAL /IED/CBR	X	X	X	LINK	
	Mail room	CBR			X	LINK	
	Control room	GENERAL /IED/CBR	X	X	X	LINK	
	infrastructure	Antiintrusion barriers	GENERAL /IED/CBR	X	X	X	LINK
		Gates	GENERAL /IED/CBR	X	X	X	LINK
		Security post	GENERAL /IED/CBR		X	X	LINK
		CCTV	GENERAL /IED/CBR	X	X	X	LINK

		CCTV face/behaviour recognition software	GENERAL /IED/CBR			X	LINK
		CCTV left item detection software	GENERAL /IED/CBR		X	X	LINK
		PA System	GENERAL /IED/CBR	X	X	X	LINK
		Ventilation protection	CBR	X	X	X	LINK
		Bollards	GENERAL /IED/CBR		X	X	LINK
		The anti-terrorism vehicle barriers	GENERAL /IED/CBR			X	LINK
		Portable temporary roadblocks	GENERAL /IED/CBR		X	X	LINK
		Access control	GENERAL /IED/CBR	X	X	X	LINK
		Unauthorized opening door and windows alarm system	GENERAL /IED/CBR	X	X	X	LINK
		Turnstile gates	GENERAL /IED/CBR			X	LINK
		Interlocking door systems	GENERAL /IED/CBR			X	LINK
	detection	Walk-through metal detectors	GENERAL /IED/CBR		X	X	LINK
		CBR detection	CBR			X	LINK
		X-Ray scanners	GENERAL /IED/CBR		X	X	LINK
		Drone support	GENERAL /IED/CBR			X	LINK
		Anti-drone system	GENERAL /IED/CBR			X	LINK

Personel									
			RISK LEVEL						
			Threat	LOW	MEDIUM	HIGH			
Security	detection	Handheld Metal detectors	GENERAL /IED/CBR	X	X	X	LINK		
		Explosives detectors	IED/CBR		X	X	LINK		
		Portable X-Ray scanners	GENERAL /IED/CBR		X	X	LINK		
		CBR detection	CBR			X	LINK		
		Inspection accessories	GENERAL /IED/CBR	X	X	X	LINK		
	protection	CBRN PPE			FFP2 mask	Mask FFP3	Full face CBR mask	LINK	
					gloves	gloves	gloves	LINK	
					googles	googles		LINK	
					personal decon. kit	personal decon. kit	personal decon. kit	LINK	
							CBRN suite	LINK	
		C-IED PPE				emergency kit	emergency kit	emergency kit	LINK
						CAT	CAT	CAT	LINK
						burn dressing	burn dressing	burn dressing	LINK
						H&L set	H&L set	H&L set	LINK
							bulletproof vest	bulletproof vest	LINK
					ballistic blanket	ballistic blanket	LINK		
					ballistic helmet	ballistic helmet	LINK		
					haemostatics dressing	LINK			

						non-flammable uniforms	LINK	
		Armed attack PPE		Coercive measures	Coercive measures	Coercive measures	LINK	
					bullet/knife proof vest	bullet/knife proof vest	LINK	
					ballistic helmet	ballistic helmet	LINK	
					ballistic blanket	ballistic blanket	LINK	
VIP/religious leaders/admin	protection	CBRN PPE		FFP2 mask	Mask FFP3	escape respiratory protection	LINK	
				gloves	gloves	gloves	LINK	
				googles	googles		LINK	
				Initial decon set	Initial decon set	Initial decon set		
		C-IED PPE				bullet proof vest	bullet proof vest	
						ballistic helmet	ballistic helmet	
		Armed attack PPE				bullet/knife proof vest	bullet/knife proof vest	
						ballistic helmet	ballistic helmet	

4. Facility security measures

Due to the diversity of the facility and its varying size, construction, and design, the facility has been divided into three areas of interest for equipment recommendations.

Area 1 – External premises of the facility.

This chapter is intended to provide a basic understanding of circuit design. It covers the location of the premises within the perimeter of the plot and the protective elements between the exterior building walls and the property boundary line. Some technical solutions also reach beyond this defined line.

Area 2 – Facility entry points/facade.

This chapter describes solutions and protection elements applicable to the building envelope including facades, entry points, and other openings and access points.

Area 3 – Internal zone.

This zone includes the internal space of the building after crossing its entry points and the security and technical infrastructure

4.1. Area 1 – External premises of the facility

4.1.1. Anti-intrusion barriers

Anti-intrusion barriers are designed to prevent unauthorized persons from entering the premises. These barriers are designed to slow down an intruder in passing an obstacle, which may result in a change of tactics in terms of gaining access and additional time for detection and response.

This role will also be fulfilled by masonry fences high enough or finished with additional features that make it difficult to get to the other side, including spikes, barbed wire, etc.

Picture 1 – Wall spikes WSF-02



Source: Shandong Xingying Environmental Energy Technology Co. LTD.,
<https://www.wall-spikes.com/wallspikes/wallspikefence.html> [access: 16.12.2022]

It can also be combined with detection devices, significantly increasing its effectiveness. These solutions mainly protect the facility in this area against theft, active shooter, and planting small IEDs.

Picture 2 & 2a – RFID perimeter protection system



Source: RCS Engineering Sp. z o.o., <https://rcse.pl/en/perimeter-protection-system/>
[access: 16.12.2022]

In order to detect unauthorized intrusion into an area protected by a fence, intrusion detectors with vibration sensors (accelerometers) are mounted directly on the fence span in configuration with a CCTV system and combined with perimetric protection of gates and gateways. Fiber optic technologies and microwave barriers are also used.

4.1.2. Landscaping

As an alternative to road barriers, the external perimeters of the facility could be planted with natural plantings in the form of trees that can stop vehicles from unauthorized entry. This solution is environmentally friendly, provides a natural look, and does not require a significant investment. The disadvantage of this solution is the time it takes for the tree to settle down and grow to the appropriate size. An added advantage is that it also provides an excellent screen from view of the property, limiting the possibility of hostile reconnaissance and remote weapon attacks. Ditches, bunds, and berms also fulfil this type of purpose.

4.1.3. Anti-ramming barriers

For the protection of pedestrians and the possibility of bringing in explosives in large quantities, it is necessary to secure external perimeters of the facility, pedestrian traffic routes, gathering places of the worshippers, and the possibility of entering the inner area of the facility by the vehicle.

The line of protection should be continuous and completely enclose the site. There should be no unprotected places where vehicles can approach or enter the site, including from adjacent plots, roads, and open areas.

For this purpose, various types of technical protections are used, which act not only as a physical barrier but also as a preventive measure and deterrent to potential attackers.

Bollards

A bollard is a small pillar used to create protective or architectural barriers. Bollards primarily serve as a visual guide, directing traffic and establishing perimeters. As landscaping features, they are available in various shapes or visually distinctive designs.

Bollards can be made from almost any material, including but not limited to the most common are metal, stone, plastic, and cement. Bollards may also be structurally constructed to physically block vehicle entry or protect individuals and assets.

There are also solutions, such as automatic retractable hydraulic bollards, which function as anti-terrorist vehicle barriers, with the possibility of hiding them entirely in the ground in order to allow the passage of vehicles at entry points and in the event of danger raising them in a short time blocking the route. This solution also makes it possible to maintain pedestrian traffic.

Picture 3 & 3a & 3b – SP 40, M50–1000 DFES bollards



Source: DFE Security Sp. z o. o., <https://www.dfes.pl/kategoria-produktu/oferta/rozba/blokady-drogowe-bollards/> [access: 16.12.2022]

The anti-terrorism vehicle barriers

This type of protection is divided into several types depending on the method of operation. Mounted on vehicle entry points to the inner area. They can be manually, automatically, pneumatically, electromechanically, or hydraulically controlled. Its primary task is to stop a terrorist attack with the use of a vehicle traveling at high speed from entering the premises, protecting against ramming the congregants and bringing into the area explosives or other dangerous substances in large quantities.

Picture 4 – Roadblocker M50



Source: DFE Security Sp. z o. o., <https://www.dfes.pl/produkt/zapora-drogowa-roadblocker-m50-dfes/> [access: 16.12.2022]

Reinforced landscape objects

Heavy objects can also be an effective barrier and complement the landscaping. These are various heavy, mostly concrete, architectural landscape objects, including benches, sculptures, and plant pots.

Picture 5 & 5a – Bollards Furniture Urban



Source: SVC Products Pty Lt., <https://svc.com.au/products/civil/concrete-pits/> [access: 16.12.2022]

Portable temporary roadblocks

These installations are not necessarily a permanent part of the facility's infrastructure but can be used as additional security measures for specific events or during high-risk periods. The advantage of this solution is the lack of significant financial outlays on the modernization of existing infrastructure and the limitation of the designated area only for a limited period. By design, these elements must meet the requirements of anti-terrorism protection.

Picture 6 & 6a – F11, F18 mobile roadblock



Source: DFE Security Sp. z o. o., <https://www.dfes.pl/kategoria-produktu/oferta/rozbaz/blokady-drogowe-bollards/bariery-tymczasowe/> [access: 16.12.2022]

Some mobile vehicle barriers that allow authorized vehicles and emergency services to pass through also meet legal requirements for escape routes and accessibility.

Picture 7 – Mobile Road Blocker



Source: Mobile Gate Security A part of Security Holding Denmark,
<https://mobilegatesecurity.com/products/mobile-roadblock/> [access: 16.12.2022]

Gates

A reliable means of access control is the entrance gate. Self-supporting sliding gates operate regardless of the characteristics of the road and its slope. Swing gates can reliably and economically secure access to the protected area. A swing gate can be used whenever a sliding gate's space is insufficient for proper operation. Some anti-terrorism gate solutions meet the appropriate security requirements and required standards.

Picture 8 – The Delta Cantilever Sliding Gate



Source: Wallace Perimeter Security., <https://www.wallaceperimetersecurity.com/gates/slide-gates/delta> [access: 16.12.2022]

4.1.4. Security post

Permanent or temporary security guard posts are constructed when there is a need to ensure the safety of a fixed location on the perimeter of a building or at vulnerable points. Security posts are designed to enhance a security guard's ability to perform their duties 24/7. The security post should also provide shelter in adverse weather conditions, provide adequate lighting, be equipped with appropriate technical support, and be protected against vehicle ramming.

Picture 9 – Colored Security Post



Source: AB Sea Container Private Ltd., <https://www.indiamart.com/proddetail/colored-security-post-17623595791.html> [access: 16.12.2022]

4.1.5. CCTV system

The primary function of the CCTV (Closed Circuit Television) system is to support and protect the facility and manage it properly. It must cover all sensitive points. In many cases, it also serves as evidence in criminal or terrorist cases and allows for accurate reconstruction of the event. Further features of this system are deterrence and prevention capabilities, where we reduce the likelihood of attack. A well-functioning security system supported by appropriate technology can detect hostile reconnaissance and prevent existing hostile activities. The system must be operated by qualified personnel, and all critical points must be well illuminated and free of so-called blind spots. The system should be designed and installed by professionals preceded by a security audit, which will guarantee its correct functioning.

Picture 10 & 10a – CCTV system



Source: Geotechnology IT Group Sp. z o.o., <https://www.geotechnology.pl/systemy-cctv/>
[access: 16.12.2022]

Face/behavior recognition system

Additional features of this system can be equipped with appropriate software and a database for face recognition. In many European countries, such a function is highly effective but limited by law.

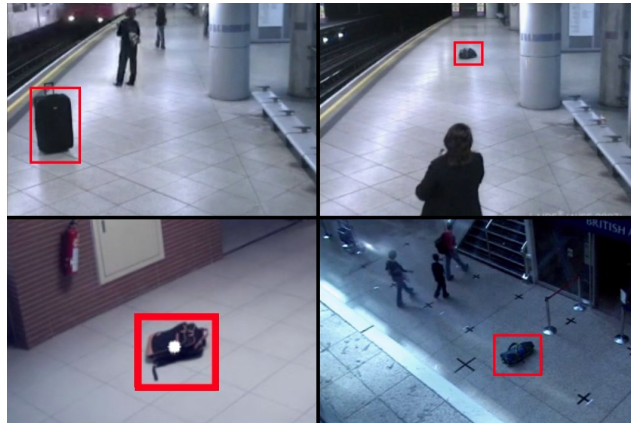
Picture 11 – Screen capture from the Skylark system



Source: Skylarklabs, Inc. <https://skylarklabs.ai/public-safety#/> [access: 16.12.2022]

Left item detection

The left-behind baggage recognition system identifies potentially dangerous objects in public spaces where terrorist threats pose a real danger. It performs its role very well in finding objects that may contain improvised explosive devices (IEDs) and CBR agents. In case of detection of the object left in the supervised area, the software automatically informs the system operator about the situation, who decides on further steps. There are also solutions for detecting unusual behavior that can detect the behavior of a potential assassin.

Picture 12 – Abandoned Luggage Detection

Source: viso.ai., <https://viso.ai/application/abandoned-luggage-detection/> [access: 16.12.2022]

Body Worn Camera

They are becoming standard equipment for security services. They affect the safety of those using them, record video and audio from incidents. They also act preventively during hostile reconnaissance. Designed to operate regardless of the existence of a permanent CCTV system.

Its use is conducive to reducing complaints about the actions of security. They have a significant impact on reducing violent incidents. Properly used, show the event and the situation from the security point of view. Together with the radio communication system, it creates an extensive surveillance system with direct preview by CCTV operators (just like drones). The recordings can provide evidence in proceedings and often constitute essential evidence in a case. It is required to prepare a number of procedures for handling recordings, including who and when can have access to recordings, to whom and on what terms copies are made available. It is also necessary to handle copies following General Data Protection Regulation.

Picture 13 – Body worn cameras

Source: Caught In The Act Video Surveillance Pty Ltd., <https://www.citact.com.au/product/body-worn-cameras/> [access: 16.12.2022]

4.1.6. Waste containers

An essential element in security system is the proper supervision, placement, and design of trash garbage cans. These are places that are naturally suited for leaving a variety of items, including dangerous objects. Therefore, they should receive special attention from security supervisors in this matter.

4.1.7. Drones solutions

Drones are increasingly supporting public services in providing security and are also exploited by criminals or terrorists. Therefore, drone support and protection against them must meet appropriate requirements.

Drones support

Flying drones are equipped with high-resolution cameras that provide real-time data of the circumscribed area of interest. The algorithms allow mapping the area by building, street, vehicle, or person. This allows for planning the event's details to ensure the participants' safety.

Picture 14 – DJI Mavic 2 Enterprise Advanced, DJI Matrice 300 RTK drones



DJI Mavic 2 Enterprise Advanced



DJI Matrice 300 RTK

Source: TPI Sp. z o.o., <https://tpi.com.pl/pl/katalog-produktow> [access: 16.12.2022]

Thanks to the technology, such devices ensure control over the crowd gathered at the event. It is possible to zoom in on the area of interest and take appropriate security protocols. The technology also enables integrating police databases with facial recognition algorithms. This solution allows for the detection of criminals or terrorists at an early stage of their planned activities.

Picture 15 – Drone recognition system screen capture from the Skylark system



Source: Skylarklabs, Inc., <https://skylarklabs.ai/public-safety#/> [access: 16.12.2022]

It is also possible to equip the drones with accessories useful during crowd control. These include megaphones, searchlights, drop systems, and communication systems.

Picture 16 – Drones accessories



Source: TPI Sp. z o.o., <https://tpi.com.pl/pl/katalog-produktowPic> [access: 16.12.2022]

To operate drones, proper qualifications are required, and drone aviation is regulated by the European Union Aviation Safety Agency (EASA), which has standardized rules among its member states - (EU) 2021/1166 of July 15, 2021.

Anti-drone systems

Antidron systems are primarily entrusted to law enforcement agencies. Appropriate national approvals must be obtained for the purchase and operation of the relevant system. By design, they are not dedicated to individual consumers because of the damage that can be done to people and property.

We can divide these devices into 3 groups:

- for military applications - laser sets, guided missiles, etc.,
- kinetic devices - net launchers (hand-held) mounted on interceptor drones,
- non-kinetic devices - mainly based on radio frequency solutions (jamming/interceptor).

Kinetic devices

Hand-held interceptor net launchers are designed to intercept flying drones at low altitudes and speeds. They fire a net that weaves into the rotors of the drone. The disadvantage of this solution is that the drone falls inertly from its height, and therefore, it has significant limitations on its application.

Picture 17 – Antidrone net muncher Sky Wall 100



Source: My Drone Services Inc., <https://mydroneservices.com/drone-mitigation-deterrent-solutions/>
[access: 16.12.2022]

Another kinetic solution is anti-drone systems launched from another drone. Depending on the solution, it can autonomously track a passing device or be controlled by an operator. This is a safe solution due to the fact that the intercepted drone remains hooked up to the capturing device.

Picture 18 – Drone Catcher - Delft Dynamics BV



Source: Delft Dynamics., <https://www.forcesoperations.com/amp/laid-a-la-recherche-dun-drone-intercepteur-de-drone/> [access: 16.12.2022]

Non-kinetic devices

Non-kinetic antidrone systems are based on electronic hardware and software. They work on the principle of detecting a flying device with the help of various types of radar, appropriate qualification, and neutralization.

Various types of radars and sensors are used for detection purposes. These include but are not limited to radars, acoustic detectors, and detection cameras, which can give a device's location with a high degree of accuracy.

Picture 19 & 19a & 19b & 19c – Anti-drone system SkyCtrl





Source: Advanced Protection Systems SA., <https://apsystems.tech/produkty/sky-ctrl/> [access: 16.12.2022]

Then, the drone is classified and assigned to the appropriate group using artificial intelligence. If the collected data determines that the flying object is unauthorized, it displays the pertinent information to the operator, who decides on further action. Once the decision is made, the operator activates neutralizing devices consisting mainly of jamming radio bands or giving appropriate commands to the device to bring it to the ground and immobilize it. Radio frequency jamming is strictly regulated by the relevant country's internal authorities.

There are also hand-held solutions, where the operator aims the interceptor at a flying object and, thanks to the installed directional antennas, sends a jamming beam in the direction of the device. When the jamming beam reaches the drone, it is possible to bring the device to the ground or command it to return to "home" or the remote-control device location.

Picture 20 – Drone interceptor gun DroneGun Tactical



Source: DroneShield LLC. <https://www.droneshield.com/dronegun-tactical> [access: 16.12.2022]

4.2. Area 2 - Facility entry points

Deterrence and detection are vital to eliminating a threat inside a building. Therefore, proper screening procedures for persons entering the building should be used. There are many technical features to streamline the inspection process. Unfortunately, they bring a number of inconveniences, such as financial outlay, uncomfortable conditions for the worshipers/visitors, additional equipment space, and technical infrastructure. Additionally, for these outlays to fulfil their role, these posts should be physically separated from the facility's interior. This should be arranged so that a potential attacker cannot get from the control zone to the location of the planned attack.

4.2.1. Entry/exit

Access control

By design, it is an electronic system for verifying and assigning access authorization to selected personnel. Several key points must be followed for the system to perform its function, and all entry points must be equipped with it. It is crucial to minimize the number of entry points, and doors equipped with it should be fitted with a self-closing system and emergency locking system in case of need. An additional advantage of this system is the possibility to designate internal zones ensuring the segregation of persons moving in a given area.

Picture 21 & 21a – Access Control Systems

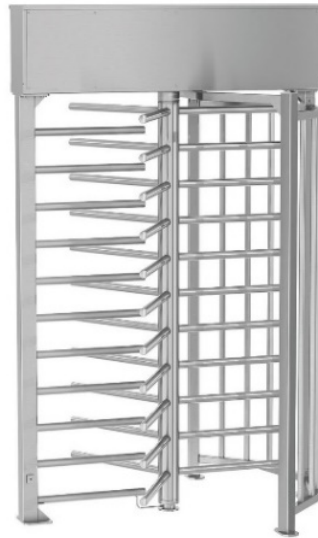


Source: Standard Telephones and Cables., <https://telephonesandcables.com/access-control-security/>
[access: 16.12.2022]

Turnstile gates

Turnstiles are installed in areas particularly prone to attack or unauthorized entry and where high throughput is a requirement. They are often integrated into an access control system or installed after a personal screening, where they can be interlocked and prevent an attacker from entering.

Picture 22 – Turnstile gate REXON ERA 3



Source: DFE Security Sp. z o. o., <https://www.dfes.pl/kategoria-produktu/oferta/rozbaz/bramki-i-furty/wysokie-furty-obrotowe/> [access: 16.12.2022]

Alternatively, smaller versions of this device are available but do not prevent access to the designated area. It is possible to pass a tripod twister over.

Picture 23 – Tripod twister Bar BA



Source: DFE Security Sp. z o. o., <https://www.dfes.pl/kategoria-produktu/oferta/rozbaz/bramki-i-furty/obrotowe-bramki-kolowrotkowe/> [access: 16.12.2022]

4.2.2. Screening and detection equipment

Handheld Metal Detectors

Hand-held metal detectors are designed to detect metal objects brought in by people on the premises. This device makes it possible to search a person without violating his/her personal rights. This device can detect metal knives, IEDs, and inspect small suitcases, packages, letters, firearms, and other objects brought into the protected area. These devices are not expensive, easy to use, and generally available.

Picture 24 – Handheld metal detector Super Scanner®V



Source: Garrett Electronics Inc., <https://garrett.com/security/hand-held/super-scanner-v-hand-held-metal-detector> [access: 16.12.2022]

Walk-through metal detectors

This is a larger version of the metal detector in the form of a gate. These devices are characterized by a high throughput than hand-held metal detectors but are associated with more significant expense, designation of the appropriate place, power supply, and additional lightning. They can be mounted for the duration of the event and quickly and easily dismantled. Often, this post is equipped with another hand-held detector to precisely locate the metal object.

Picture 25 – Garret Walk-thru metal detector



Source: Garrett Electronics Inc., <https://garrett.com/security/walk-through> [access: 16.12.2022]

Both solutions are associated with using an additional table for searching things brought into the area of the object and a workplace for security personnel.

X-Ray scanners

Stationary X-ray scanners are used primarily where there is an increased risk of a terrorist attack. These devices generate X-rays that travel from a source to a receiver, analyzing differences in the density of objects placed between them. These devices are expensive, and the operation requires specialized training. It also requires considerable space and adequate infrastructure to be considered during its installation. The advantage of this system is the possibility to precisely inspect the contents of objects without opening them, even placed inside solid objects, electronic equipment, closed boxes, and items sealed in factory packaging. In some devices, installed software supports the operator's ability to identify prohibited items and devices such as weapons or IEDs. Thanks to the applied technical solutions, they also distinguish between organic and inorganic compounds, significantly affecting the detection capabilities of explosives and some chemical and biological agents.

Picture 26 – X-ray scanner



Source: Safeway Inspection System Ltd., <https://www.safeway-system.com/What-should-be-paid-attention-to-when-using-x-ray-baggage-scanner-id3375671.html> [access: 16.12.2022]

Modern solutions also make it possible to manually scan suspected items. During the scanning process, thanks to the technology used, the scanner is slowly moving scanned object without contact, and generates two-dimensional image in real-time on a high-resolution color display.

Picture 27 – Handheld X-ray scanner NIGHTHAWK



Source: Z&Z Biztonságtechnika Kft., <https://znz.hu/termek/viken-hbi-hordozhato-visszaszoraso-keziroentgen-backscatter/> [access: 16.12.2022]

Explosives detectors

Explosive detectors can be divided into several groups depending on the amount of material to be sampled, the technology used, the physical state of the sample, and its mobility. They are used to detect homemade, commercial as well as military explosives. Depending on the technology used, some devices take vapours samples from the air or directly from the tested surface with swabs. Some solutions combine both technologies. Various colorimetric tests are also based on the reaction of corresponding solutions with explosives and are expressed by a colour change on the corresponding paper. These devices are relatively cheap and easy to use. The disadvantage is that the sample must be taken directly from the test substance or swabbed. Electronic devices are expensive and trigger the appropriate safety procedures more often. The advantages of these devices include detection capabilities to detect even trace amounts of explosives, even after a considerable period following exposure to the explosive. A wide range of available devices allows you to tailor solutions to the conditions and requirements of the facility.

Picture 28 – ENTRYSCAN® 4 - high-sensitivity high explosives walk-through detection system



Source: Rapiscan Systems., <https://www.rapiscansystems.com/en/products/entryscan>
[access: 16.12.2022]

Picture 29 – Smiths Detection SABRE 5000 chemical trace detector



Source: Federal Resources, <https://www.federalresources.com/product/sabre-5000/>
[access: 16.12.2022]

Picture 30 – IONSCAN™ 500DT - simultaneous explosives and narcotics trace detector



Source: Smiths Detection Group Ltd., <https://www.smithsdetection.com/products/ionscan-500dt-2/> [access: 16.12.2022]

Picture 31 – Ultra™ Multi-Target Explosives & Precursors Test Kit



Source: Ideal Blasting Supply Inc., <https://idealblasting.com/ultra-multi-target-explosives-precursors-test-kits-box-of-10/> [access: 16.12.2022]

CBR detectors

The detection of CBR substances involves specialized knowledge and high-quality equipment dedicated exclusively to this hazard group. Detecting substances expose the operator to hazards and exposure. Testing without additional personal protection equipment is a lethal risk, which is why the equipment is dedicated mainly to specialized services. Despite this, a number of detection devices are available on the market without special permission, regulated by the internal regulations of a particular country or by internal company policy. These devices very often have additional explosives detection capabilities. A relatively less expensive alternative to expensive and customer-restricted devices are toxic industry chemicals detectors which are limited to chemicals detection abilities. It does not change the fact that testing a sample requires exposure to a hazardous agent.

Chemical detectors

As with explosives detection, several types of devices are divided into groups depending on the technology used, the amount of material to be sampled, the physical state of the sample, and its mobility. In facilities producing or using toxic industrial substances in the production process, dedicated detectors for specific contaminants are installed. Chemical hazards can also be identified using a chemical detection method. In this case, the chemical compounds react with the corresponding reagents, which results in a change of color.

Picture 32 – Gemini™ Combining Raman and FTIR technology Chemical Analyzer



Source: Delta Science., <https://www.deltasciencemm.com/category/portable-analytical-instruments/>
[access: 16.12.2022]

Picture 33 – RAID-M100 Plus - Ion Mobility Spectrometry (IMS) hand-held Chemical Agent detector



Source: Bruker Corporation., <https://www.bruker.com/en/products-and-solutions/cbrne-detectors/ims/raid-m-100.html> [access: 16.12.2022]

Picture 34 – Dräger Detection Tubes



Source: Drägerwerk AG & Co., https://www.draeger.com/en_uk/Products/Sampling-Tubes-and-Systems [access: 16.12.2022]

Biological detectors

Rapid detection is critical in minimizing the effects of biological weapons use. In many cases, the first symptoms occur a considerable time after exposure to the threat. Detection and identification of this type of hazard should take place in specialized labs and be performed by appropriately trained and protected personnel. Nevertheless, rapid and accurate detection is the key to minimizing the effects of biological agents in terrorist acts.

Picture 35 – BioCheck™ Powder Screening Test Kit



Source: 20/20 Gene Systems. <https://2020gene.com/home-page/> [access: 16.12.2022]

Picture 36 – Qubit™ 3 Fluorometer

Source: Fisher Scientific AG., <https://www.fishersci.ch/shop/products/qubit-3-0-quantitation-starter-kit/15397463> [access: 16.12.2022]

Radiation detectors

Detection of ionizing radiation and radioactive materials is impossible without appropriate equipment that detects its presence, type of radiation, its intensity, which allows estimating the level of risk for humans. Basic detectors for detecting ionizing radiation and dose meters are relatively inexpensive and widely available. False alarms are rare with this type of device and are mainly caused by human maintenance errors. These solutions can be installed at entry points to facilities, used as hand-held detectors, or as personal equipment for employees as dosimeters that measure the received radiation dose.

Picture 37 – NeutronRAE-II - personal radiation detector

Source: Gastech Australia Pty Ltd (Gastech), <https://gastech.com/products/radiation-monitoring/neutronrae-ii> [access: 16.12.2022]

Picture 38 – X-Ray and Gamma Personal Dosimeters PM1610A

Source: Polimaster Europe UAB., <https://polimaster.com/eu/product/x-ray-and-gamma-radiation-dosimeters/personal-dosimeters/personal-dosimeter-pm1610/> [access: 16.12.2022]

4.2.3. Unauthorized opening door and windows alarm system

Detectors and devices that indicate an unauthorized entry attempt by rule are part of the anti-intrusion system. These devices should operate in a 24-hour system in places that should be permanently closed (such as emergency exit doors, back rooms, and key technical rooms of the facility). Additionally, such a system should have a possibility of temporary authorization for entering and leaving so that it does not cause false alarms during the operating hours of a given zone. Such sensors are mounted on any door or window that can be used as an entry point to a facility. They are usually magnetic or mechanical switches connected to the alarm system. These are low-cost alarm systems and do not represent a significant investment at the construction stage. In the case of already existing buildings, there is a need to connect sensors by wire (which should be prospected), which can be a technical problem. The disadvantage of this solution is that the sensor can be bypassed, for example, by breaking and going through the glass of a window. Therefore, the design and installation should be commissioned to a professional company that provides for such a possibility by installing additional technical protection. Wireless versions are also available, but they involve changing the battery and using a wireless network.

Picture 39 – Open/Close Alarm Sensor for SCW Shield - 74WOS

Source: Security Camera Warehouse., <https://www.getscw.com/window-alarm-sensor> [access: 16.12.2022]

4.2.4. Interlocking door systems

This system is installed at access points to critical and sensitive places. It can be installed in small rooms or as a security booth, consisting of two doors with monitored and controlled locks. It is not possible to open two doors at the same time. The doors are controlled in two ways, one is by an operator who authorizes the person by visual inspection, and the second is automated using a key card or PIN code. In this type of solution, there is a possibility of stopping a suspect inside the room.

Picture 40 – Man Trap Doors - Standard Telephones and Cables



Source: Standard Telephones and Cables., <https://telephonesandcables.com/access-control-security/>
[access: 16.12.2022]

4.2.5. Signage

Proper signage indicating specific evacuation routes, assembly points, safe havens, etc., will increase the effectiveness of the emergency response. Appropriate signage on access roads guarantees smooth traffic flow and indicates places or areas designated for emergency services, e.g., fire roads, hydrant locations, assembly points, etc. On the other hand, avoid designating security-sensitive locations such as command posts, CCTV rooms, critical objects, and infrastructure. An adequately marked facility is a great help to people unfamiliar with its topography, and often in emergency situations, it is the only indicator of safety procedures to be followed. Signage also has the additional benefit of sending clear and strong deterring signals to potential attackers that the facility is appropriately manned and secured. It can also protect against hostile reconnaissance, where the person gathering information about the facility is aware that he/she is being recorded. The recording can be used in the investigative process.

Picture 41 – Surveillance Cameras In Use Signe



Source: Discount Safety Signs Australia, <https://www.discountssafety signsaustralia.com.au/products/security-signs/surveillance-cameras-in-use/> [access: 16.12.2022]

4.2.6. Facade

The façade of a building is a barrier that separates the outside from the inside with numerous entry points, windows, columns, and other functional elements of the structure. In places of worship, it is also, in many cases, a decorative element of the building itself, which can amplify its effects during an attack with high explosives.

To ensure that a structure is adequately resilient to the effects associated with the detonation of a high explosive charge, it must be considered at the building design stage following applicable safety standards (appendix. No. 1).

To ensure the safety of buildings not designed for this type of hazard, create a buffer zone to provide a stand-off distance. The stand-off distance is defined as the distance between the detonation and the protecting building (the bigger, the better).

Mostly related to large IEDs (mostly VBIEDs) that may create primary and secondary fragmentation from the blast. When the blast accrues shatters the glass in windows (glass walls), causing the large fragments to fall, creating structural damages and fragmentation. This is why this consideration should be taken for buildings facades for the mass event congregation. This can be done using the measures described above to prevent the vehicle from entering directly under the facility facade.

4.2.7. Doors, glazing, and windows

Door

In addition to their standard purpose, doors in buildings can perform many additional functions, such as anti-burglary, ballistic, fire, weather protection, etc. However, they must maintain their primary function.

The doors of the facility should be appropriate to the potential hazard. Other than in the case of the building structure itself, they can be modernized in existing door openings in most cases.

In the context of security, they function as the first barrier an assassin may encounter in his path during a forcible entry. Therefore, it is a good solution to consider installing a burglar-proof door or changing the locks and door bolts to burglar-proof. This allows to slow down or prevent force entry, even using tools or firearms.

In addition to entry points into the facility, these doors should also be provided for special purpose rooms (safe houses, control rooms, vaults, etc.). Doors and locks shall be certified and meet the latest security standards depending on their resistance class (see appendix no. 1). Also, they should be installed by qualified personnel who install them based on a detailed design using proven and certified test methods, following other safety regulations. Only such installation guarantees their correct functioning at an adequate resistance level.

These solutions do not represent a significant financial outlay but significantly reduce the vulnerability to potential aggressors.

In the case of increased risk of explosives or firearms use, there are solutions to protect also in this aspect. Due to appropriate technical parameters of door openings, the installation of such doors must be preceded by a proper specialist analysis of the possibility of their application.

Picture 42 & 42a – Burglar resistance door and lock



Source: Shield 100 Ltd., <https://www.shield-security-doors.co.uk/> [access: 16.12.2022]

Glazing and windows

Windows, glazing, and stained glass are important functional and architectural elements of each building. Damage caused by accidents, natural weather phenomena, or terrorist attacks can produce significant amounts of glass fragments. Such incidents can cause numerous injuries and deaths to the worshippers both inside and outside the building. Therefore, they should remain under special supervision and adapted to the existing risks.

Detonation blast-resistant windows

Explosion-proof windows are installed to eliminate or reduce casualties from the explosive charge detonation and the resulting high-velocity glass shards. The greater the hazard and other circumstances that increase the risk level (e.g., a small stand-off distance from the street), the higher the level of blast protection the window should be provided. Due to the standards that must be met by the window and its installation (see Appendix no.1), the application of such a solution should be assigned to specialized companies that will adapt protection requirements to the threat and technical capabilities of the object. Installation of this type of protection is expensive and will not always be possible, but it provides adequate protection against explosion hazards.

Picture 43 – Blast Resistant Windows



Source: Window Gard B.V., <https://windowgard-security.com/index.php/blast/15-blast-resistant-windows> [access: 16.12.2022]

Antifragmentation film

The substitute of the detonation blast-resistant windows is the use of a protective film installed on the window glass. This solution can reduce the danger from explosion by keeping glass shards together. Furthermore, the mechanical film attachment to the window frame reduces the risk of the glass being pulled out of the frame during the negative pressure.

An added benefit is protection from thrown objects. It effectively stops even heavy, low-speed objects from falling inside and protects against glass fragments. This solution is inexpensive, effective against thrown objects, and somewhat reduces the effects of the detonation of the explosive charge.

Picture 44 – Safety and Security Window Films



Source: EUROLAB., <https://www.laboratuvar.org/pl/testler/otomotiv-testleri/ece-r-43-motorlu-tasitlarin-guvenlik-cami-onayi/> [access: 16.12.2022]

Forced entry resistant/anti-burglary windows

Security windows should be used primarily where they are easily accessible from the outside, especially from a level directly accessible from the ground or structural or terrain elevations.

Similar to the door, they should be certified and meet the latest security standards depending on their resistance class (see appendix no. 1). In addition, they should be installed by qualified personnel who install them based on a detailed design using proven and certified test methods, following other safety regulations. Only such installation guarantees their correct functioning at an adequate resistance level. Installations of this safety measure make it difficult or impossible to overcome even using tools, and this significantly reduces the risk of an attacker getting through this entry point. They are characterized by a reinforced frame, built-in anti-ramming mechanisms, locks in the handles, and laminated or polycarbonate glass. This solution is relatively cheap and can be installed in most existing facilities.

Picture 45 – Anti-burglary window



Source: Oknoplast Sp. z o.o., <https://oknoplast.com.pl/dawka-wiedzy/okna-bariera-dla-zlodzieja/>
[access: 16.12.2022]

Bars

Bars are an effective solution against forcible entry through the windows. They are installed in window openings or other facility access points. Correctly installed, they are a significant obstacle that an attacker needs tools and time to break through. High efficiency, adaptability to existing window openings, and low costs are the advantages of this solution. Unfortunately, they also have limitations in the application, mainly due to fire and evacuation regulations.

4.3. Area 3 - Internal zone

4.3.1. Safe room

A safe room is a designed or adopted room that serves as a shelter in an emergency. Provides shelter to its occupants from such threats as armed aggressors, the detonation of explosives, firearms, chemical threats, fire, and natural disasters. They can be divided into designed/adopted facilities (safe rooms) or temporary shelters that provide temporary short-term protection (shelter-in-place). Shelter-in-place is a low-cost solution for rooms that are not permanent occupancy facilities but only shelter until a safe evacuation can be possible.

In addition to standard protection, there are dedicated solutions for CBR threats. Mainly by using appropriate filtration in the ventilation system or by switching it off. It is possible to equip a standard shelter with proper PPE to give the possibility of surviving an attack. To meet the best of its requirements, the room should start at the building design stage. Adapting an existing room is possible but can be complicated and expensive (especially for CBRN threats). Such rooms can also protect against armed attack or hijacking, but this solution requires the facility to be equipped with walls, doors, and windows ballistic protection.

Shelter location and capacity are crucial in the space design process. Another critical element to consider are escape routes. They should be easily accessible and properly marked. The time and the distance to travel to reach the shelter should also be considered. Such shelters should also meet requirements for people with disabilities. Such a room should be equipped appropriately depending on the expected time to ensure its independence from external factors. Most importantly, it should be equipped with water, food, sanitation, medical supplies, communications equipment, and additional survival gear.

All these elements should be properly selected by a qualified company.

4.3.2. Mailroom

To counter the dangers of shipments containing hazardous substances and devices, there is a separate room for their inspection. There are two types of threats identified. These are explosive and CBR threats. Every facility should provide temporary or permanent dedicated mail room, especially when preparing for a mass event. An alternative solution is redirecting mail to a specialized company for verification and security checks. The receiving and screening room should be in a location with minimal risk to few. The best solution is to locate this facility outside critical areas, away from the main entry point and other vital assets. In the event of a bomb threat, such a room should be designed to allow positive pressure to escape outside the building. In addition, with this type of hazard, it is important to equip it with explosive-resistant containers. The structure itself should provide sufficient safety in the adjacent rooms. In the case of increased hazards, the room should also be equipped with detection equipment for the anticipated risks. It should additionally be equipped with personal protective equipment appropriate to the anticipated hazard.

Picture 46 – Mailsafe Bomb Box

Source: bombrieven.nl., <https://www.bombrieven.nl/product/mailsafe-bomb-box/> [access: 16.12.2022]

4.3.3. Control room

The monitoring room (control room) is critical in ensuring facility security's efficient and effective management. It is where information is gathered and flows between security officers and other employees. From this place, evacuation and rescue operations should be coordinated. There are control panels for all security systems (CCTV, intrusion, fire protection, access control, BSM (building management system), PA (public address system)). It is also a surveillance point for vehicle traffic in all zones and for people entering the site. In order to manage the security, the room must be properly equipped and protected against unauthorized access.

For this room to meet its requirements, it must be designed, located, and equipped by a professional company and meet current quality standards according to the following principles:

- the room cannot serve a dual function, e.g., detention room, mail reception, record storage,
- should be located away from traffic routes accessible to the public,
- should be isolated from installations that may affect its operation,
- should be able to manage critical building control systems,
- should ensure ergonomics and efficiency for the CCTV monitoring operator,
- should additionally be equipped with personal protective equipment (PPE) appropriate to the anticipated hazard and suitable for managing any type of incident,
- should be equipped with a separate communication line with a direct connection to the critical points of the facility,
- should have a backup power supply to keep essential systems running at full capacity,
- equipped with extinguishing agents that do not damage or interfere with the operation of the equipment,
- arming doors with appropriate resistance depending on the anticipated threat, access control system, two-way videophone system,
- equipping the room with a surveillance camera.

4.3.4. Public address/voice alarm system

During an emergency, clear and precise voice messages are essential to effective safety management. Public address/voice alarm system delivers pre-recording voice warning messages. It also provides an effective method of communicating critical information and emergency instructions. It enables the effective, calm, and controlled management of staff and other people on the premises. The system can be divided into several zones, which makes it possible to inform and instruct the relevant groups of people in given areas, which is an important part of security management. It also does not cause unnecessary panic.

It consists of an integrated IP network, input controllers, and a speaker network system. It may also combine the microphone for announcements and message recordings.

Picture 47 – Public Address, Bosch Security and Safety Systems



Source: DSI sp. z o.o., <http://www.dsintegracje.pl/aktualnosci/nowosc-paviro-bosch.html>
[access: 16.12.2022]

The detailed scope of its deployment and uploaded or prepared commands depends on the facility's risk analysis and response plan. As this technology underpinning the incident detection and signaling infrastructure continues to evolve, the standards for how this system should operate are increasing. Commands and instructions may vary depending on the emergency and need. The public address system may emit specific or default tones, broadcast priority voice commands according to established codes, or hazard-specific commands. Compared to traditional alarm methods such as alarm bells or voice commands, the response time to a threat is significantly improved.

4.3.5. Panic button

Panic buttons are devices used to signal a robbery or other event related to a security threat to people or property. There are loud and silent alarms depending on the procedure adopted in the safety documentation and the situation. Such pushbuttons may be either stationary (placed in high-risk rooms/places such as security posts, main entrance points, reception area, church pulpit, etc.) or mobile, the equipment of persons responsible for the security of the facility. Such devices are usually connected to the facility's primary alarm system and activate the structure of notification and alarming according to the established safety chain.

They can be installed in wired or wireless versions. The remote control is very convenient and easy to use. The standard range in the open space is about 200 m (differs indoors, dependent on building structure), but there are also models with a much longer range. The remote control is available as a

one or multi-channel model. In the multi-channel version, the radio channel can be used to trigger a panic alarm (loud or silent), and the remaining channels can be used for such purposes as a garage door, a parking barrier, or other safety features. They can be paired with almost any alarm system and utility automation. They require little investment and are easy to apply to alarm installations.

Picture 48 & 48a – Panic button



Source: Security Alarm Corp., <https://www.securityalarm.com/blog/does-your-bank-need-a-panic-button/> [access: 16.12.2022]

4.3.6. Integration systems - Physical Security Information Management (PSIM)

As part of the interconnection of various independent systems related to facility management and security, integration systems are installed. Depending on the version used, these solutions enable integration with any number of security or building automation systems through dedicated interfaces. In advanced versions, it is possible to connect any number of sensors and define any number of procedures and situational plans.

Mobile versions are also installed on mobile devices, extending the system's functionality by managing resources such as mobile patrols, services, emergency services, etc. This is a particularly useful feature during terrorist events where a major command post or management point is rendered inoperable (in case of a full evacuation, command post takeover, use of CBR agents, etc.).

Picture 49 – Physical Security Information Management system - GEMOS MOBILE



Source: Ela-compil sp. z o.o., <https://ela.pl/2016/12/07/aplikacja-gemos-mobile/> [access: 16.12.2022]

The main benefits of its use are:

- quick and easy assignment of tasks to mobile devices,
- efficient management of resources (patrols, technical services, emergency services, etc.),
- position tracking in open terrain and inside buildings,
- immediate information on the violation or exceeding the designated zones,
- reporting with the possibility of attaching multimedia documentation.

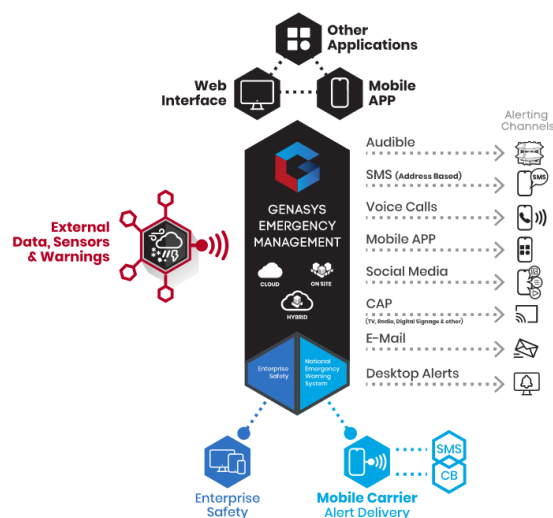
4.3.7. Integrated Mass Notification System

Integrated Mass Notification System enables public safety and enterprise operators to quickly and effectively alerts and notifications across multiple channels from a single unified command and control interface to help keep employees and individuals safe.

The system can assist with:

- zone creation - preplanning to create specified zones and routes for evacuation,
- evacuation and planning - build zone-based evacuation plans including population, structure, traffic, and other data (past events, local knowledge, and known potential local hazards),
- fire protection - incident occurs and all communities/zones are alerted on where to go,
- operator - receives alerts and warnings on easy-to-use dashboard and activates notifications,
- mobile alerts - send geotargeted SMS, Text, Cell Broadcast, Email, and Social Media,
- voice notifications - broadcast audible sirens and clearly understood voice messages over local or large areas.

Picture 50 – Genasys Integrated Mass Notification System



Source: Genasys™, <https://eu.genasys.com/es/gestion-de-emergencias-genasys/>
[access: 16.12.2022]

4.3.8. Critical utility infrastructure

Some technical installations are critical infrastructure for the facility's daily operation but may also be critical during an evacuation. Such installations should also be designed in locations less vulnerable to attack.

To protect the facility's technical infrastructure, keep signage at these locations to a minimum. They should be protected with fencing, access control, detection devices, and vegetation to conceal above-ground systems.

Ventilation system

A mechanical ventilation system provides a constant supply of fresh air to indoor areas and removes used air, regardless of atmospheric conditions. Depending on the object's size, it may operate as a single system or a network of independent centers.

The most vulnerable components are air intakes, handling units, and ducts.

A system potentially exposed to the hazards of spraying chemicals, biological agents, or suspensions that emit ionizing radiation. Properly securing access to the technical space ensures that equipment and the transmission network are protected from the immediate risk of contamination.

In many existing buildings, air intakes are located below or a ground level. Locating the intake at the highest practical level of the building is desirable. To protect against the hostile activity, air intakes should be shielded, monitored, and inaccessible to the public.

A proper filtration system is also used to protect against accidents or terrorist attacks. Air containing hazardous gases, vapours, and aerosols must be appropriately filtered to meet its requirements. This is mainly achieved by passing the air through various types of filters and absorbers. The most common way to purify the air from aerosols are mechanical filters and chemical/mechanical absorbents for vapours and gases.

Due to the high investment and maintenance costs, this solution is mainly used in safe rooms.

Detectors for chemical and biological agents in ventilation systems are also used to improve safety. Detection devices for biological hazards are less common, expensive, and the detection time is extended. These devices also require specialized operation and specialized personnel. Due to a large number of potentially hazardous chemicals, it is recommended to install equipment capable of detecting the most probable ones (e.g., in case of hazards caused by industrial installations of nearby plants).

Water supply

Water infrastructure, along with the technology necessary to operate it on a daily basis, is considered one of the most critical components of technical infrastructure. Thus, it can be contaminated by introducing poisons, pathogens, or chemicals into the distribution systems.

Access to points in the system where chemical or biological agents can be introduced sufficiently to cause health risks should be limited and accessible only to facility maintenance personnel. In addition, where water treatment is used, the range of chemical and biological contamination should be periodically controlled.

Emergency power supply

Emergency power, lighting, and backups for all critical systems allow security systems continue to operate during emergency situations (e.g., when the security control room is damaged or during a power failure). The emergency power system should be designed in such a way as to provide electricity only to the most critical elements of the building's safety equipment.

This can be accomplished in several ways by installing battery backup power, UPC systems, and emergency power generators. These systems are often interconnected to increase reliability and continuity of power supply.

5. First response equipment

In order to ensure an efficient, safe, and effective response to emergency situations and awareness of implemented procedures, it is necessary to provide additional emergency equipment for the personnel managing the facility's security. A well-designed, equipped, and properly located package will significantly increase the effectiveness of emergency response actions. Personnel responsible for coordinating emergency actions should be familiar with its contents, location and trained in its use.

5.1. PPE

Personal protective equipment (PPE) is worn to minimize exposure to hazards that cause injury and illness.

5.1.1. CBRN PPE

PPE is individual, specialized equipment and clothing for employees to ensure protection from hazardous conditions (such as chemical agents, biology agents, and toxins). General work clothing (such as suits, pants, and shirts) is not considered PPE. While using the specific PPE required is determined by a risk assessment. To prevent the effects of a terrorist attack using CBR agents, the goal should be to protect as effectively as possible against all hypothetical scenarios. When selecting appropriate PPE, size is a crucial criterion, and choosing the right size of equipment ensures that its properties are maintained. Further considerations affecting the effectiveness of the protection are the use of compatible PPE (masks, goggles, overalls, gloves), proper sealing of joints so that they form a tight unit, proper training in dressing and undressing.

CBRN PPE Levels

Vapours, gases, and particulates from hazardous substance response activities place response personnel at risk. For this reason, response personnel must wear appropriate personal protective clothing and equipment whenever they are near the site. The more that is known about the hazards at a release site, the easier it becomes to select personal protective equipment. There are four levels of personal protective equipment.

Level A protection is required when the greatest potential for exposure to hazards exists, and when the greatest level of skin, respiratory, and eye protection is required. Examples of Level A clothing and equipment include:

- positive pressure, full face-piece self-contained breathing apparatus (SCBA) or positive pressure supplied air respirator with escape SCBA,
- totally encapsulated chemical and vapor-protective suit,
- inner and outer chemical-resistant gloves.

Level B protection is required under circumstances requiring the highest level of respiratory protection, with lesser level of skin protection. At most abandoned outdoor hazardous waste sites, ambient atmospheric vapours or gas levels have not approached sufficiently high concentrations to warrant level A protection. Examples of Level B protection include:

- positive pressure, full face-piece self-contained breathing apparatus (SCBA) or positive pressure supplied air respirator with escape SCBA,
- inner and outer chemical-resistant gloves,

- face shield,
- hooded chemical resistant clothing (impermeable),
- coveralls,
- outer chemical-resistant boots.

Level C protection is required when the concentration and type of airborne substances is known and the criteria for using air purifying respirators is met. Typical Level C equipment includes:

- full-face air purifying respirators,
- inner and outer chemical-resistant gloves,
- hard hat,
- escape mask,
- disposable chemical-resistant outer boots.

Level D protection is the minimum protection required. Level D protection may be sufficient when no contaminants are present or work operations preclude splashes, immersion, or the potential for unexpected inhalation or contact with hazardous levels of chemicals. Appropriate Level D protective equipment may include:

- gloves,
- coveralls,
- safety glasses,
- face shield,
- chemical-resistant, steel-toe boots or shoes.

While these are general guidelines for typical equipment to be used in certain circumstances, other combinations of protective equipment may be more appropriate, depending upon specific site characteristics.

Eye protection

These should provide eye protection from chemical and biological splashes and protect against dust. By design, goggles and safety glasses should have protective shields on the sides to prevent these substances from entering the eye in angled splash situations. Prescription goggles are also available in specialized stores.

Eye protection is often integrated with face masks, which provide the best protection.

Protective glasses do not provide full protection against dust, vapours, and aerosols entering the eye, therefore suitable protective goggles are recommended. The best goggles are made of soft components that ensure a tight fit with a properly curved surface that fits the face.

Picture 51 & 51a – Dräger X-pect® 8100 Cover Spectacles, Dräger X-pect® 8500 protective goggles

Source: Dräger Polska Sp. z o.o., https://www.draeger.com/pl_pl/Productselector/Head-and-Eye-Protection/Protective-Eyewear?page=1 [access: 16.12.2022]

Respiratory Protection

Respiratory protection protects personnel from inhaling airborne hazardous substances in various forms (aerosols, liquid/solid particles, gases, or vapors).

There are many possible hazards associated with improper use of respiratory protection. To avoid these, it is important to remember:

- improper fitting and wearing of a respirator mask - a mask cannot fully protect if it does not properly fit the face,
- touching the inside of a respirator mask can result in the transfer of contamination and eventually lead to substances entering the mouth and nose,
- taking unnecessary risks of exposure by users as a result of a false sense of protection - it is always better to maintain an appropriate stand-off distance.

There are three types of respiratory protection:

- air purifying masks,
- self-contained breathing equipment,
- rescue and Escape Apparatuses.

Air purifying masks - filtering half-masks, full-face masks, filtering masks with forced circulation.

These solutions depend on the air in the given environment and filter it of hazardous substances. Depending on the environment, they can be used if the oxygen content is at the appropriate level (a minimum of 17%) and the type of hazardous substance is known (only a suitable filter can ensure proper functioning). Therefore, it is recommended to use masks with filters of the broadest possible spectrum:

- single-use half-masks - recommended filtration class FFP3/P3/N99/N100 - they do not protect against most chemical substances and are mainly used in case of biological risks, they protect against harmful dust and aerosols, including carcinogenic and radioactive substances and pathogenic substances such as viruses, bacteria, and fungal spores,

Picture 52 – Dräger X-plore® 1900 dust mask



Source: Dräger Polska Sp. z o.o., https://www.draeger.com/pl_pl/Products/X-plore-1900
[access: 16.12.2022]

- reusable respirators half-masks with replaceable filters - depending on the type and filters used, can be a good solution for respiratory protection in some cases of CBRN hazards,

Picture 53 – MSA Comfo Classic® Half-Mask Respirator



Source: MSA Safety Incorporated, <https://us.msasafety.com/Air-Purifying-Respirators-%28APR%29/Elastomeric-Half-Masks/Comfo-Classic%C2%AE-Half-Mask-Respirator/p/000100000200001030> [access: 16.12.2022]

- full-face masks - provide respiratory and eye protection at the same time. They are available in one- or two-filter versions.

Picture 54 – Dräger CDR 4500 full-face mask



Source: Dräger Polska Sp. z o.o., https://www.draeger.com/pl_pl/Products/CDR4500 [access: 16.12.2022]

Self-contained breathing equipment - used mainly in places with oxygen content below 17% or where there is a dangerous concentration of hazardous substances. This solution provides a constant supply of air or oxygen and is an independent breathing apparatus. When used correctly, it gives complete protection against the effects of CBR agents. These devices require periodic technical inspections, and the personnel using them must undergo appropriate medical examinations and training.

Picture 55 – G1 SCBA Self-contained breathing apparatus



Source: MSA Safety Incorporated, <https://pl.msasafety.com/Aparaty-oddechowe-na-spr%C4%99%C5%BConie-powietrze/Aparaty-oddechowe-na-spr%C4%99%C5%BConie-powietrze/G1-zintegrowany-aparat-powietrzny/p/00> [access: 16.12.2022]

Rescue and Escape Apparatuses

These are used in emergency situations to provide immediate protection from harmful agents for a limited period.

There are:

- devices dependent on atmospheric air - these are fire and industrial escape hoods with installed efficient filter absorbers designed to protect against toxic gases, vapours, and industrial and fire particles, providing adequate filtration for a minimum period of 15 minutes; these devices are dependent on atmospheric oxygen.

Picture 56 & 56a – Dräger PARAT® 4700 escape hoods



Source: Dräger Polska Sp. z o.o., https://www.draeger.com/pl_pl/Products/PARAT-4700 [access: 16.12.2022]

- equipment independent of ambient air:
 - compressed air apparatus - these are systems that provide a continuous supply of air for a minimum of 15 minutes from a compressed air cylinder and come in the form of a full-face positive-pressure mask or escape hood,
 - regenerative oxygen devices - ensuring access to oxygen in conditions of toxic gases and lack of oxygen in a given environment; depending on the version, they provide air supply for up to 60 minutes.

Picture 57 – Dräger Saver PP Emergency Escape Breathing Apparatus



Source: Dräger Polska Sp. z o.o., https://www.draeger.com/pl_pl/Products/Saver-PP
[access: 16.12.2022]

Picture 58 & 58a – Dräger Oxy K 30 H escape devices



Source: Dräger Slovenija d.o.o., https://www.draeger.com/en_seeur/Products/Oxy-K-30-S-HW-HS
[access: 16.12.2022]

Safety Gloves

Provide an additional element of protection for overall safety management personnel. It should be used whenever a CBRN incident is suspected. They must meet a number of requirements, should be resistant to chemical and biological substances, abrasion-resistant and other damage, and thin enough not to hinder manual activities. Therefore, their proper selection is crucial to ensure adequate protection for the employee. In principle, double-dressed pairs of gloves should be used during CBRN incidents. This primarily protects against secondary contamination when undressing after decontamination and provides extra protection against damage to the top protective layer.

The most universal and ensuring adequate protection are nitrile protective gloves 0.2 - 0.4 mm thick, characterized by appropriate chemical and biological resistance, mechanical resistance, antistatic properties, and do not significantly interfere with manual activities.

Picture 59 – Safety gloves table

„Latex“ Gloves	Nitrile Gloves	Vinyl Gloves
<p>Latex gloves are natural material, made from natural rubber – rubber tree.</p> <p>They are a popular choice of protective glove for medical or industrial use.</p> <p>The primary reason people would choose an alternative to latex is because many people suffer from latex allergies.</p> <p>When allergy is not a concern, latex does have a slight advantage with comfort and dexterity over nitrile gloves.</p>	<p>Nitrile gloves are made out of a synthetic rubber, and are an ideal alternative when latex allergies are of concern.</p> <p>Nitrile gloves are the superior glove when it comes to puncture resistance. Nitrile gloves are often referred to as “medical grade.”</p> <p>Before gloves can be marketed to hospitals and medical institutions, they must undergo a series of tests conducted by the Food and Drug Administration (FDA) to ensure their durability.</p>	<p>Vinyl gloves are a popular choice for the food industry and situations where high levels of durability and protection are less of a priority.</p> <p>While they may be less durable, they are the less expensive option.</p>
<p>Fit like a second skin</p> <p>Have a high level of touch sensitivity</p> <p>Are good for wearing for an extended amount of time</p> <p>Work well for high-risk situations involving infectious material</p> <p>Are cost-effective</p> <p>Are lightly powdered, making it easier to put on</p> <p>Are very elastic and strong</p> <p>Are biodegradable</p>	<p>Latex-free</p> <p>Are most puncture resistant</p> <p>Have a high level of sensitivity</p> <p>Mold to your hand for a great fit</p> <p>Are good for wearing an extended amount of time</p> <p>Work well for high-risk situations involving infectious material</p> <p>Resist many chemicals</p> <p>Have a long shelf life</p> <p>Are available in blue or black to help identify if the glove has been punctured</p>	<p>Latex-free</p> <p>Have a looser fit</p> <p>Are good for short-term, low-risk tasks</p> <p>Are the most economic option</p> <p>Have anti-static properties</p> <p>Are best for use with non-hazardous materials</p> <p>Are lightly powdered to make it easier to put on”</p>

Source: ISEMI – International Security and Emergency Management Institute

Protective clothing

Protective clothing is a barrier between harmful external factors and human skin. Depending on application and danger, it is divided into categories:

- Category I - providing protection against minimal danger,
- Category II - provides protection against specific factors that do not threaten life and health,
- Category III - protection against external factors dangerous to life and health.

The suits of the highest protection category are divided into subcategories (type 1-6). They are made of materials ensuring an adequate chemical and biological protection and are light and comfortable.

Picture 60 – Protective clothing table

Type	Description	Relevant standard
1a-B, 1b-B, 1c-B	Gas tight	EN 943-1:2002, EN 943-2:2002
2-B	Non gas tight	EN 943-1:2002, EN 943-2:2002
3-B*	Protection against pressurised liquid chemicals	EN 14605:2005 + A1:2009
4-B	Protection against liquid aerosols (spray tight)	EN 14605:2005 + A1:2009
5-B	Protection against airborne solid particulates	EN ISO 13982-1:2004+ A1:2010
6-B	Limited protection against liquid chemicals (light spray)	EN 13034:2005 + A1:2009

Source: ISEMI – International Security and Emergency Management Institute

The most universal suits for non-professionals are suits meeting requirements for Type 4B clothing (protection against pressurized liquid jets and biological agents). Additional equipment includes shoe protectors and an integrated protective hood. Proper sizing, training in dressing and undressing are essential to ensure adequate protection.

Picture 61 – Protective suit 3M 4570

Source: 3M Marketplace, https://www.3m.com/3M/en_US/p/d/b00046817/ [access: 16.12.2022]

Initial decontamination

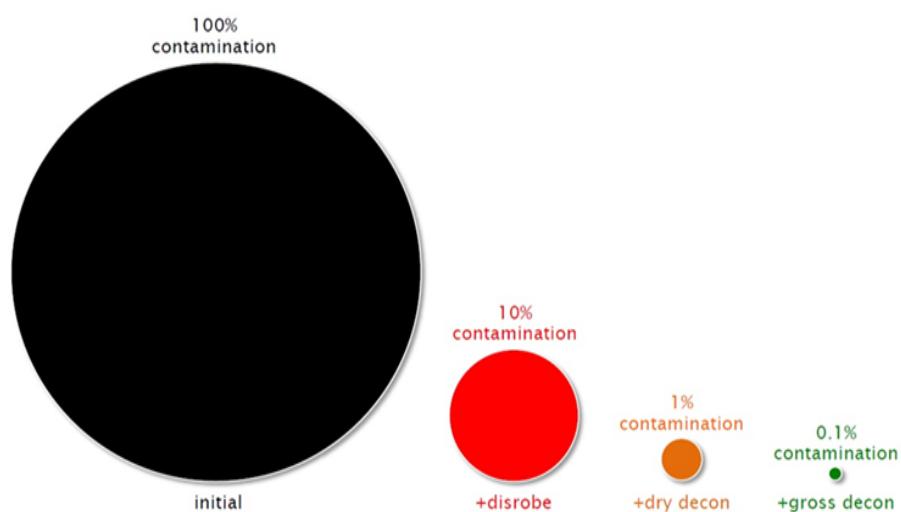
Decontamination removes the hazardous substances from the victims, the responders and their PPE, and the equipment and vehicles at the chemical incident site.

The aim of decontamination is to prevent the movement of hazardous substances from contaminated into clean areas and to protect the public and downstream responders from

exposure by secondary contamination, and to protect emergency responders by decreasing the stress on their PPE.

There is a very useful rule to remember regarding decontamination: the so-called 'rule of tens'. This rule states that the rapid and effective completion of each decontamination stage (disrobe, dry, and wet decontamination) leads to a ten-fold reduction in the level of casualty contamination. So, each stage reduces the amount of contamination and the risk to the casualty and first and second responders. Dry decontamination are any available dry, absorbent materials that can be used, for example: kitchen towels, toilet rolls, or paper tissues, such as 'blue roll' towels and clean rags, strips of blanket, or sheeting. Other absorbent materials like dry soil or cat litter can also be used. Wet decontamination using water should only be used for decontamination where the chemicals are confirmed as being caustic or corrosive or if the individual is displaying signs and symptoms consistent with exposure to caustic substances. It requires minimal equipment and training in the Rinse-WipeRinse procedure.

Picture 62 – CBRN response stages



... rapid and effective completion of each stage of the incident response procedure yields a ten-fold reduction in the level of casualty contamination

Source: ISEMI – International Security and Emergency Management Institute

Technic decontamination is the planned and systematic process of reducing contamination to A level that is as low as reasonably achievable (ALARA).

- Technical DECON is a multi-step process in which contaminated individuals are cleansed with the assistance of trained personnel,
- technical DECON is similar to a car wash
- there is an entry point and an exit point (I.E., the DECON line).

Picture 63 & 63a – Decontamination process

Source: ISEMI – International Security and Emergency Management Institute

There are many technical solutions providing decontamination of personal, equipment or vehicles as well as internal and external subphases. One of them is made by the company Cristanini which provides the full set of decontamination solutions, jet generators, decontamination vacuum cleaners, or personal decontamination tents.

Picture 64 – Decontamination equipment

Source: ISEMI – International Security and Emergency Management Institute

Initial decontamination kits (PDKITs) are ready-to-use lightweight sets for removing or neutralizing CBR agents from people or equipment. It is not a replacement for complete decontamination but only a first response to the threat to minimize the exposure to hazardous agents until the arrival of professional emergency services. It is recommended to use this solution where the CBRN risk is increased. The most important in such a case is the time of contact of the hazardous substance with the skin. Immediate application of such a kit reduces the risk of severe burns and prevents the number of dangerous substances from being absorbed into the body.

Regardless of the type of hazard (chemical, biological, radiological), the personnel conducting decontamination should be familiar with and trained in its use. The decontamination kits were designed for soldiers involved in warfare to maintain their combat capability. Some of the kits intended for military use are also designed and dedicated to the civilian community. The kits are usually packed in a

hermetically sealed package and consist mainly of decontaminating mitts, solutions, and lotions used to remove, absorb, or neutralize the agent. The more extensive kits contain a number of additional items to assist and enhance the decontamination process:

- poncho with hood,
- cotton briefs (pants),
- elastic knitted socks,
- plastic shoes such as beach sandals,
- protective half-mask,
- moist non-woven towel,
- moist hygienic glove for washing exposed parts of the body,
- identification bands marked with an individual number,
- plastic bag for contaminated clothing and waste,
- plastic bag for personal items,
- disposable nitrile gloves.

Picture 65 – RSDL® Reactive Skin Decontamination Lotion Kit



Source: Emergent BioSolutions Inc., <https://www.rsd.com/about-rsd/> [access: 16.12.2022]

Picture 66 – Skin decontamination by RSDL sponge



Source: https://www.researchgate.net/figure/Skin-decontamination-by-RSDL-sponge_fig3_294424232
[access: 16.12.2022]

5.1.2. C-IED/Armed attack PPEC-IED/Armed attack PPE

In order to protect key personnel, including those responsible for security and evacuation operations, it is recommended to equip them with measures that provide adequate protection against the IEDs detonation effects, gunfire, or stabbings. Ballistic vests are used for this purpose.

Anti-stabbing vest

A stab vest is a protective element worn under or over outer clothing to protect against stabs and other sharp objects to a person's chest, back, and sides. They are made of high-density and strength synthetic fibers such as Kevlar. Puncture resistance is defined in, but not limited to, NIJ 0115.00 and is expressed on a three-grade scale depending on the ability to protect against a knife or spike measured in joules.

- Level 1- 24 joules,
- Level 2- 33 joules,
- Level 3-43 joules.

In most cases, Level 1 protection is sufficient against most knife attacks. Some solutions give resistance to needle and spikes attacks.

Picture 67 – Hercules Covert Stab, Spike and Needle Resistant Vest



Source: Body Armour Canada Ltd., <https://www.bodyarmourcanada.com/shop-bullet-resistant-or-stab-resistant/covert-stab-spike-and-needle-resistant-vest> [access: 16.12.2022]

Bullet and fragmentation-resistant vests

The protective vest, also known as a ballistic vest or a bullet/fragmentation-resistant vest has become the essential equipment of every law enforcement officer. It is increasingly being used by security guards and facility security staff.

The ballistic and fragmentation resistant vest protects not only from small arms projectiles and fragmentation but also from knives and spikes.

The vest absorbs the impact and reduces the penetration of bullets or fragments from detonation.

It is made of high-density and strength multilayer fabric woven of synthetic fibers such as Kevlar. Such inserts are sewn or inserted into a cover sewn into the shape of a vest. To increase the resistance of certain parts of the vest, they are equipped with additional reinforcement in the form of ballistic plates. They are made of various materials resistant to high-energy bullets such as metal, ceramics, and resistant plastics such as polyethylene, placed in pockets to protect the body's main organs.

Are available in many resistance classes as defined by the appropriate standards. The most common standard is NIJ standard 0101.06.

Additional constructional features of the vest increasing its protection area are collars and crotch or shoulder protectors. They are also made of elastic ballistic inserts, mainly Kevlar.

Picture 68 – Ace Link Armor MSOV Modular



Source: ACE Link Industrial Inc. <https://acelinkarmor.com/m-s-o-v-modular-special-operations-vest-flexcore/> [access: 16.12.2022]

Picture 69 – DFNDR Armor Lightweight Level III+ armour plate



Source: DFNDR ARMOR a Division Of Engense Inc. <https://dfndrarmor.com/products/level-iii-pp-rifled-body-armor> [access: 16.12.2022]

Ballistic blanket

These blankets are made of high-quality soft ballistic material such as Kevlar and are similar to bulletproof vests, providing shrapnel protection following relevant standards. They are highly maneuverable due to foldability and flexibility, so they can be used in various tactical situations, such as in vehicles, to cover walls, doors, people, etc. Because they are collapsible, they do not take up much space and can be, to some extent, effective protection against firearms or the effects of an IED detonation.

Picture 70 & 70a – Ballistic blanket

Source: BSST GmbH, <https://www.bsst.de/en/de02.html> [access: 16.12.2022]

Head protection

Head protection systems include ballistic helmets, hybrid solutions, and helmets, along with complementary modules that, when properly selected, create a total solution to protect people's heads from a wide range of threats. Ballistic helmets are most commonly used for head protection against firearms hazards and IED detonation effects. Other versions do not provide adequate protection. They are most often made of compressed Kevlar and high-resistance synthetic materials such as reinforced ballistic polyethylene. Such structures must meet stringent protective standards depending on the resistance required. The most common standard for helmets is NIJ 0106.01. The helmet can be equipped with additional accessories to ensure easy installation of the various modules, which include side mounting rails (for mounting flashlights and other accessories) with flexible cables with a hook to stabilize the night vision goggles, a front mount with a socket for night vision, garda and an optional selection of accessories kit designed for specific needs. The whole thing is supported on the head with the help of a fascia.

Picture 71 & 71a – Galvion helmet VIPER P4

Source: Ha3o, <https://sprzetspecjalny.pl/produkt/helm-viper-p4/> [access: 16.12.2022]

Flame-resistance clothing

Flame-resistance clothing is used where there is a risk of fire or explosion. It does not provide long-lasting protection against open flames or high temperatures, and its use is intended to minimize the effects created during a fire or IED detonation. Thanks to the use of suitable fibers, the flame is not sustained and extinguishes itself. Notably, the fibers do not melt but glow, which does not cause the melted fibers to stick to the skin, significantly reducing the depth of burns and shortening the recovery period. Additional flame-resistant equipment completing the overall protection are gloves and non-flammable balaclavas. They come in many versions, and they appear like ordinary outerwear from the outside.

Picture 72 & 72a – QS24 - Nomex® Comfort – Dupont Flame-resistance clothing



Source: uPont de Nemours, Inc., <https://www.dupont.com/products/dupont-nomex-bulwark-gs24.html> [access: 16.12.2022]

Combat application tourniquet

It is a disposable compact system for temporarily stopping severe bleeding from body extremities.

It is a fabric band placed on the limb and twisted until the bleeding stops. It is used for dressing wounds after gunshots, amputations, and wounds sustained after an IED explosion. A correct application does not require extensive training and can be limited to reading the manual. It contributes significantly to reducing fatalities and the deterioration of the condition of the injured until professional assistance is provided at the hospital.

The advantage of this solution is the possibility of self-application with one hand.

Picture 73 – C-A-T® GEN7 - CAT Resources combat application tourniquet

Source: TacMed Australia, <https://tacmedaustralia.com.au/collections/workplace-response/products/cat-tourniquet> [access: 16.12.2022]

Burn dressing

Pre-hospital cooling therapy is a well-established first aid treatment for burns. Effective use of cooling can reduce the extent and depth of tissue damage and pain. Most commercially available burn kits are based on water therapy. The water gel dressing principle of operation is based on the flow of heat from the wound to the gel, which is more effective than cooling the wound with water (it is aseptic, stays on the skin, gives a surface protection, does not lead to excessive tissue cooling or hypothermia, easy to open, easy to remove without pain for the victim, available in multiple sizes and shapes).

Depending on the chosen solution, it can be used in 1st, 2nd, and 3rd-degree burns. It should be a component of first-aid kits for hazards related to detonation of IEDs or fire.

Picture 74 – Burn dressing Water-Jel Technologies

Source: CVN Medical Solution, <https://www.cvn.fi/en/osasto/burn-injuries/> [access: 16.12.2022]

Hemostatic dressing

Hemostatic dressings are designed to inhibit hemorrhage in arterial injuries of various origins. These include firearm wounds, post-blast wounds, cuts, traffic accidents, and many others. It works by blood coagulation and expands the gel inside the dressing to form a gel "plug". This ensures the seal of the wound and inhibits the flow of blood. Such dressings are germicidal, thus protecting the wound from infection. The disadvantage of such a dressing is the knowledge of providing the first aid for this type of wound. To stop bleeding it is necessary to find the bleeding location in the wound, dry it and apply the dressing, often deep inside the wound. Therefore, it is recommended to apply it only after proper training.

Picture 75 – Hemostatic dressing CELOX RAPID



Source: Medtrade Products Limited, <https://medtrade.co.uk/mtproducts/celox-rapid/>
[access: 16.12.2022]

Accessories – Inspection mirror/cameras

Cameras and inspection mirrors are integral attributes of security personnel. As the inspection mirrors are dedicated mainly to controlling entering vehicles, and in smaller versions to check hard-to-reach places in buildings, the inspection camera allows viewing objects being brought into the premises. Inspection cameras can be used to inspect incoming packages, items, and hard-to-reach objects without damaging or opening them. It is often possible to drill a small inspection hole to gain access to the inspection camera. The device consists of an integrated camera on a flexible probe connected to a digital display. These devices have a built-in camera, LED light, high-resolution color display, and sometimes an infrared light source. It is possible to record video and take high-resolution images for further analysis.

Picture 76 – Inspection cameras RIDGID CA-350X



Source: Emerson Electric Co., <https://www.ridgid.eu/pl/pl/kamera-inspekcyjna-micro-ca350x> [access: 16.12.2022]

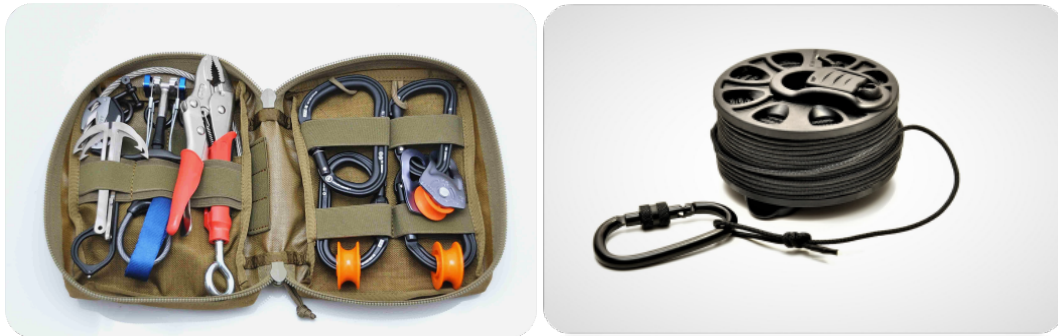
Picture 77 – TSS Under Vehicle Search Mirror, Range: 4 Inspection mirror



Source: ANGEL GIL LEMOS, <https://espiando.es/detectores/detector-explosivos/espejo-de-inspeccion-convexo-anti-explosivos-vision-bajo-vehiculo-linterna-led-y-bolsa-de-transporte/> [access: 16.12.2022]

Accessories – Hook and line set

This kit is a basic set of simple tools for remote displacement or opening various types of objects in case of suspected hazardous content. It is useful mainly in places where there is no possibility to support law enforcement agents or when there is no time to call for support. The most basic version consists of a line and a hook, but it can be extended with a number of other valuable accessories (wood screws, duct tape, climbing loops, self-grip pliers, blocks, snatch blocks, etc.). Using this set significantly increases the safety of the person manipulating the object. It increases the stand-off distance and, with the use of blocks, can be operated from a safe place. Such a basic kit requires training in hazard recognition and tactics, techniques and procedures for its use.

Picture 78 & 78a – Hook and line kit

Source: own photos. Author: Dominik Klimas

Emergency kit

Emergency equipment should include all necessary means to support operations during emergency situations. The best solution is to collect all the necessary accessories into one bag and place them in the facility in designated areas accessible to security personnel. Such packages may include, but are not limited to:

- emergency instructions,
- individual flashlight,
- multitool,
- chemical lights - to mark zones (safe/dangerous - green/red),
- emergency communication kit,
- reflective vests with emergency instructions,
- first aid kit,
- CBRN PPE,
- PDKITs,
- warning tapes,
- reinforced duct tape,
- thermal blankets,
- biological waste bags or CBR waste bags.

6. Conclusions

Religious sites are considered to be especially vulnerable to attacks due to their accessibility and the fact that there are usually limited security measures applied. The equipment recommendations in the document are only part of the measures and solutions that affect the improvement of the security level, particularly deterrence, detection, prevention, and response to potential attack attempts, personal protection, and CBR threats. As part of the technological evolution, it is essential to maintain a constant ability to monitor the market and technological innovations that can significantly increase the effectiveness of prevention or protection while reducing costs for the user.

The technical sophistication of some solutions in this document raises several challenges for the end user in effectively exploiting the potential of the selected equipment.

Firstly, the complicated handling and the method of preparing the equipment for operation require comprehensive training for those dedicated to working with such specialized tools.

Secondly, the operation of some equipment requires appropriate permits. It enforces constant supervision of adherence to operating conditions, including storing in proper conditions (often in rooms dedicated to the equipment), maintaining adequate charge levels of power sources, and supplementing necessary accessories.

Finally, and thirdly, maintaining constant service supervision of these tools/devices, as is dictated by manufacturers' recommendations and inherently related to this, scheduling additional budgeting to provide funds for these purposes.

Using devices and their application in local conditions has a distinct role in the security of religious sites.

All this means that to fully secure against the entire spectrum of terrorist threats, a place of worship would have to transform itself into a specialized security unit, which would be associated with substantial financial and personnel expenses.

Therefore, it is crucial that, as part of the considerations before selecting appropriate equipment options, consultations should be held with representatives of local LEAs, for a proper assessment of the site's vulnerability to particular forms of terrorist attacks. Consultation and later equipment selection decisions are also important regarding the time of response to situations by emergency services. Knowing how a site can protect itself speeds up response to incidents and eliminates mistakes in assessing the situation at early stages by local services.

A proper relationship with local services also brings additional benefits. With good cooperation with LEAs, municipalities and others, worship places can significantly improve their security, especially in the context of organized mass events.

It should be emphasized that the key element of our efforts under the PROSPERES project is the protection of people who are in such places. The presented solutions, despite their universal nature, do not focus, for example, on the protection of property, but on the safety of people.

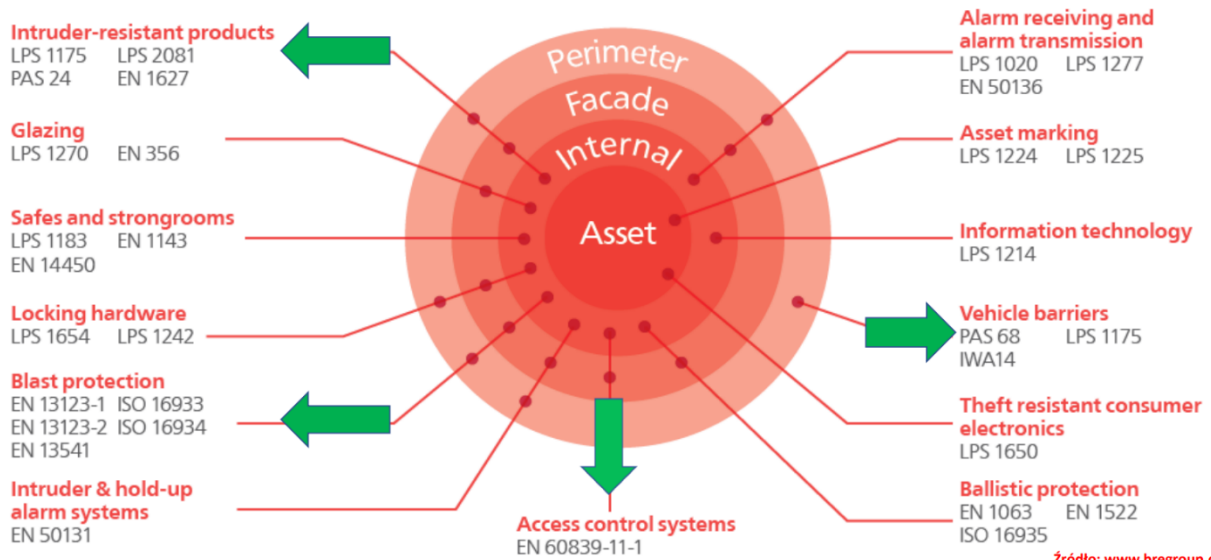
List of References

Note:

Third party images have been used in this work in accordance with applicable fair use provisions for educational and demonstration purposes only. Relevant copyright or other rights apply accordingly. References to third party products are not recommendations or endorsements.

- CBRNPol “Students Handbook”
- SECURE “CBRN security manager handbook”, Łódź 2018
- Risk Management Series “Safe Rooms and Shelters Protecting People Against Terrorist Attacks” FEMA 453, May 2006,
- Beyond Concrete Barriers Innovation in Urban Furniture and Security in Public Space, January 2018
- Explosives Trace Detectors (ETDs) Market Survey Report November 2021, US Department of Homeland Security
- Personal Decontamination Kits Market Survey Report SAVER T MSR 14 APPROVED FOR PUBLIC RELEASE, US Department of Homeland Security, February 2017
- Buildings and Infrastructure Protection Series, Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings, US Department of Homeland Security, October 2011
- Guidelines for Enhancing Building Security In Singapore, Joint Operations Group - Ministry of Home Affairs,
- Weapons Technical Intelligence (WTI) Improvised Explosive Device (IED) Lexicon - 4th Edition, Joint IED Defeat Organization, J5 Division, October 2012

Appendix A





prosperes.eu



This project is funded by the European Union's
Internal Security Fund – Police under Grant
Agreement No. 101034230 – ProSPeReS



The protocols for communication and cooperation with public services

Appendix 3

of GUIDEBOOK on security measures for religious sites & communities

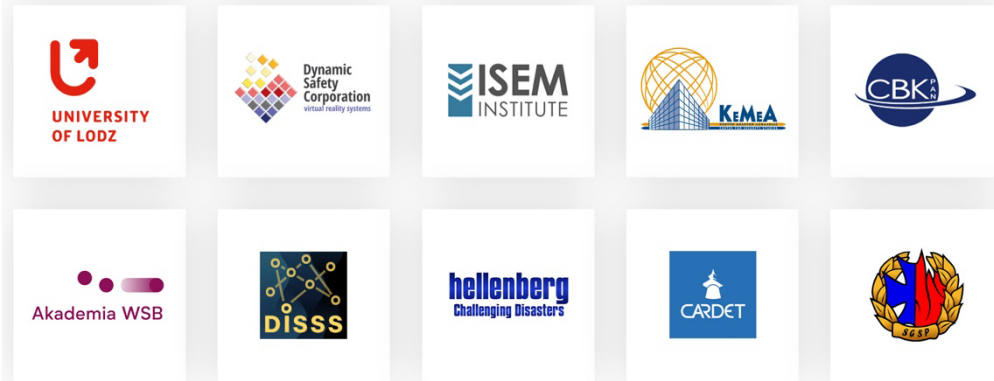


This project is funded by the European Union's Internal Security Fund – Police under Grant Agreement No. 101034230 – ProSPeReS

prosperes.eu

ProSPeReS consortium

Security experts, security research and academic institutions, providers of technical solutions and services



Law enforcement agencies (LEAs)



Faith-based organizations



The protocols for communication and cooperation with public services

Appendix 3
of GUIDEBOOK on security measures
for religious sites & communities

Document description

WP number and title	WP3 – Preparing the tailor-made security measures for religious sites; A.3.5 – Preparing protocols for communication and cooperation with public services
Lead Beneficiary/Author(s)	SGSP (Wiktor Gawroński, Marcin Smolarkiewicz, Tomasz Zwęgliński, Łukasz Faralisz)
Contributor(s)/Author(s)	UL, CBK, WSB, HP, KWPL, KWPW, WMP and other partners
Document type	Report
Last Update	08/03/2023
Dissemination level	Public / Confidential *

* Confidential – only for members of the consortium & EC Services

Acknowledgement:

This project is funded by the European Union's Internal Security Fund — Police. Grant Agreement No. 101034230 — ProSPeReS

Disclaimer:

The content of this document 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.



This work is licensed under the Creative Commons Attribution 4.0 International Licence. To view a copy of this license, visit creativecommons.org/licenses/by/4.0/ with relevant national copyright provisions to be applied accordingly.

The material for this publication was developed and reviewed by ProSPeReS consortium:

No	Partner organization name	Short Name	Country
1	UNIVERSITY OF LODZ	UL	PL
2	DYNAMIC SAFETY CORPORATION	DSC	PL
3	INTERNATIONAL SECURITY AND EMERGENCY MANAGEMENT INSTITUTE	ISEMI	SK
4	CENTER FOR SECURITY STUDIES	KEMEA	GR
5	WSB ACADEMY	WSB	PL
6	STICHTING DUTCH INSTITUTE FOR SAFE AND SECURE SPACE	DISSS	NL
7	HELLENBERG INTERNATIONAL	HELLENBERG	FI
8	CENTRE FOR THE ADVANCEMENT OF RESEARCH & DEVELOPMENT IN EDUCATIONAL TECHNOLOGY LIMITED	CARDET	CY
9	ARCHDIOCESE OF LODZ	Archdiocese Lodz	PL
10	SOCIAL OBSERVATORY FOUNDATION	Social Obser.	PL
11	HOLY METROPOLIS OF IOANNINA	HMI	GR
12	JEWISH COMMUNITY OF WARSAW	GWZ Warsaw	PL
13	LODZ VOIVODESHIP POLICE	KWP Lodz	PL
14	WARSAW METROPOLITAN POLICE	KSP	PL
15	WROCLAW VOIVODESHIP POLICE	KWP Wroclaw	PL
16	HELLENIC POLICE	HP	GR
17	SPACE RESEARCH CENTRE POLISH ACADEMY OF SCIENCE	CBK PAN	PL
18	THE MAIN SCHOOL OF FIRE SERVICE	SGSP	PL

Table of Contents

Table of Figures	7
Definitions	8
Introduction	9
1. Guidelines and dedicated protocols for reporting threats and updates in the case of various dangerous situations	10
2. A model example of cooperation at the action scene of the religious sites	14
3. Models for cooperation and notification in large scale religious events	19

Table of Figures

Figure 1 – Possible indicators of a CBRN incident	12
Figure 2 – Religious event’s stakeholders	14
Figure 3 – Law enforcement agencies possible roles in religious event.....	15
Figure 4 – Fire & rescue service possible roles in religious event	16
Figure 5 – Place of worship staff information possessed and necessary – planning phase.....	20
Figure 6 – LEA information possessed and necessary – planning phase.....	21
Figure 7 – Fire & rescue services information possessed and necessary – planning phase.....	22
Figure 8 – Information possessed by place of worship staff vs information necessary by LEA and fire & rescue services – planning phase	23
Figure 9 – Place of worship staff information possessed and necessary – initial response phase	24
Figure 10 – LEA information possessed and necessary – initial response phase	25
Figure 11 – Fire & rescue information possessed and necessary – initial response phase	26
Figure 12 – Information possessed by place of worship staff vs information necessary by LEA and fire & rescue services – initial response phase.....	27

Definitions

Terms	Description
CBRN-E	<i>Chemical, Biological, Radiological, Nuclear, Explosive (substances and agents)</i>
CCTV	<i>Close Circuit Television</i>
EU	<i>European Union</i>
FAA	<i>Firearms Attack</i>
IED	<i>Improvised Explosive Device</i>
LEA	<i>Law Enforcement Agency</i>
PBIED	<i>Person- Borne Improvised Explosive Device</i>
ProSPeReS	<i>Protection System for large gatherings of People in Religious Sites</i>
PW	<i>Place of Worship</i>
UAV	<i>Unmanned Aerial Vehicle</i>
UAVIED	<i>Unmanned Aerial Vehicle (borne) Improvised Explosive Device</i>
VBIED	<i>Vehicle- Borne Improvised Explosive Device</i>

Introduction

ISO 31000:2018 Risk Management-Guidelines defines a stakeholder as a person or an organization that can affect or be affected by an event, or who has the perception that a decision or an activity connected to event might affect him/her/it. The main stakeholders related to a potential operation at the scene of religious sites that are expected to cooperate there, these are law enforcement agencies (LEA), emergency services as well as the religious sites' authorities (administrators). Having said that the emergency services cover foremost fire brigades and emergency medical services¹.

Diverse involvement of emergency services can be envisaged depending on the nature of a religious gathering. In **the most cases of religious gatherings** both, the fire brigade and the medical services, will operate routinely. It means that they are on a standby mode located in their bases and trigger the response, if necessary, after receiving a call for response from the standard emergency number (e.g. 112 centre) that is forwarded through dedicated operational software (or if other means e.g. phone call). On the other hand, **in case of large scale religious events**, comparable to mass events, special measures are taken in advance. The following ones might be enlisted: presence of paramedics among the worshippers, first aid posts set, pre-deployment and allocation of emergency services resources in the proximity of to the event site, etc. In addition for **extraordinary gatherings**, like World Youth Days, it is common that a on-site command post as well as dedicated emergency services (e.g. fire brigade) command posts at local and higher levels HQs are established. These emergency services command posts should cooperate with LEA's command posts (e.g. via liaison officers) and other stakeholders.

The cooperation between LEA's and the religious sites' authorities might be very different as the religious gatherings themselves. There is no a standard, representative religious event or even location. The place of worship might be a single standing alone building or a complex different facilities including even multi-store buildings. Large scale religious events might be conducted as an indoor or outdoor gathering. All in all, LEAs' involvement in such events protection should be adequate to identified threats and risks potentially triggered by these threats. Based on the Polish partners (KWP Lodz, KWP Wroclaw, KSP, GWZ Warsaw) opinions in this respect collected in the course of in-depth discussions, it is fair to conclude that relatively wide spectrum of approaches might be in place as it comes to the modus-operandi of such events protection.

In case of the Roman Catholic Church there is a moderate level of cooperation between Police and religious sites. Such situation mainly concerns ordinary religious ceremonies, regardless the number of participants, even for relatively large number of people taking part. Annual Corpus Christi ceremony might be an example while the Police contribution mainly comes down to the measures related to the road safety (e.g. blocking public roads where the procession walks through). On the other hand for major, extraordinary religious events, cooperation with the Police starts already at the planning stage. In such cases a representative of the curia (catholic church body) usually is appointed in order to facilitate the process of cooperation with the Police.

A different approach is implemented by the Jewish Community of Warsaw (GWZ) which invest into regular contact with the Warsaw Police HQs. GWZ has its own internal and external armed security guards, knowing the objects (including security systems) and the specificity of the rituals. Moreover, there is a research group set up that aims at browsing the internet prior large religious events. GWZ stays constantly in touch with other Jewish Communities in the country and abroad, sharing and receiving information (also in alert mode) on potential threats and incidents that could happen or have happened to the other, above mentioned communities. There are some other examples of measures undertaken by the community in place. Among them there are daily pyrotechnic checks of objects, exercises organized by the community (incl. participation of counter-terrorism Police teams), dedicated crisis rooms (incl. the main and alternative one) as well as appointed members of a crisis team in advance. Obviously, all these aspects increase the sense of security and readiness.

¹ PRoTECT Project (2021). D4.4 – Protection of public spaces: Manual for EU. Retrieved on May 24th, 2022. Source: https://protect-cities.eu/wp-content/uploads/2021/09/PRoTECT_D4.4_Final_v3.00.pdf

1. Guidelines and dedicated protocols for reporting threats and updates in the case of various dangerous situations

An emergency or other dangerous situation can happen in different phase and time of the religious event. It might be in particular firearms attack, sharp object attack, vehicle attack, IED- explosives, PBIED- explosives, UAVIED- drone, VBIED- explosives, CBRN. Regardless of the type of threat, it is necessary to pass information about it to the appropriate entities as soon as possible. It is likely that in case of an emergency, many witnesses will attempt to inform the emergency services by the EU common emergency number 112 (or different local emergency numbers if exist). It does not change the fact that the organizer should stick to an emergency response plan, if one has been developed, nevertheless as a stand-alone document or a part of any other more general plan prepared due to the event. Such type of an emergency response plan should have been agreed, and ideally trained, with LEA's and emergency services in advance. Some part of the content there, should have been dedicated to description of communication means and channels through which information flow is expected to be conveyed, especially between the organizer and key stakeholders such as first responders suitable for a threat (incl. the Police, emergency medical service, fire brigade, etc.). In order to avoid delays in providing information or its incompleteness, it should be done by a designated responsible person on the side of the organizer (e.g. a priest, an imam, a rabbi, etc., or if appointed, an incident manager). This person should be known to the rest of the PW (or event) staff and should be informed about any threats or symptoms by worshipers, welcoming team or other organizer's (security) services if they have been created. In most cases, notification must follow the country's standard procedures.

In case of firearms attack, sharp object attack, vehicle attack, explosion, it is immediately clear that a threat has occurred. An ETHANE structure of report might be used to provide proper information²:

E – exact location;

T – type of incident;

H – hazards present or suspected;

A – access – routes that are safe to use;

N – number, type, severity of casualties;

E – emergency services present and those required.

The operator of the emergency number accepting the report uses the procedure that is enlisted below³:

- the exact address or location of the incident scene;
- main reason for the call (situation);
- the telephone number and personal data of the caller.

² An ETHANE structured report is described in GUIDE for incident managers of terrorist/extremist threats and attacks which is the part of ProSPeReS document Set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks

³ <https://www.duw.pl/czk/cpr-112/aktualnosci-112/17363,Centrum-Powiadamiania-Ratunkowego-czesto-zadawane-pytania.html>; Rozporządzenie Ministra Zdrowia z dnia 19 sierpnia 2019 r. w sprawie ramowych procedur obsługi zgłoszeń alarmowych i powiadomień o zdarzeniach przez dyspozytora medycznego (Dz. U. z 2019 r. poz. 1703)

While providing the first responders agency with an address or location of an incident, it is relevant to inform about the best possible way of accessing the scene including potential physical obstacles. Moreover, it is to be remembered that rescue vehicles are the size of a truck.

When reporting the situation, be aware that crucial information is the characteristics of incident (what actually happened), number of injured persons or victims.

Additionally in case of firearms attack make it clear when you report the situation. Do not forget to tell how many terrorist appear, how they look like. If possible describe the firearm. Accept potential injured or victims report the number of hostages.

IED-explosives or other bomb threats (suspicious items) should always be taken seriously. Depending on the type of an incident, notifying the Police there should be following information provided:

- the content of the conversation with the caller who informed the PW about the hazard (a piece of paper and pencil during incoming call gives you opportunity to collect as many details as possible);
- the content of the sent message (e-mail);
- location and description of a localized item that may contain an explosive;
- the telephone number from which the call is being conducted and your name.

There are national procedures⁴ how to behave when a bomb threat occurs. Moreover, there is also a set of procedures provided in frames of the ProSPeReS project that inform and give examples of how to deal with such extreme situations⁵.

Following the procedure published by the Polish Ministry of the Interior and Administration when you receive the call:

- stay calm and don't hang up;
- if possible, signal others to listen to the telephone conversation as well;
- ask for notification of this situation to the administrator of the PW and the Police;
- note the number if the telephone handset identifies the caller number;
- write down the words of information carefully, record the conversation, if possible;
- keep the caller on the line as long as possible, use an interview form, if available, to help you collect as much information as possible (sample information from the form to collect: where is the bomb now(?), what a bomb looks like(?), which could cause an explosion(?), exact content of the statement; caller's gender; age; description of the caller voice; noise in the background);
- be available and ready to provide detailed information regarding the interview to the arriving LEA and emergency services.

⁴ For example such procedure is published by Polish Mistry of the Interior and Administration in the Internet: <https://www.gov.pl/attachment/a0b0c901-675f-41bc-ae53-22647d490b0c>

⁵ ACTIONS to take when a suspicious item of mail, package, substance is discovered, ACTIONS to take if a bomb threat-hoax is received, ACTIONS to take when a suspicious item is discovered are the part of ProSPeReS document Set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks

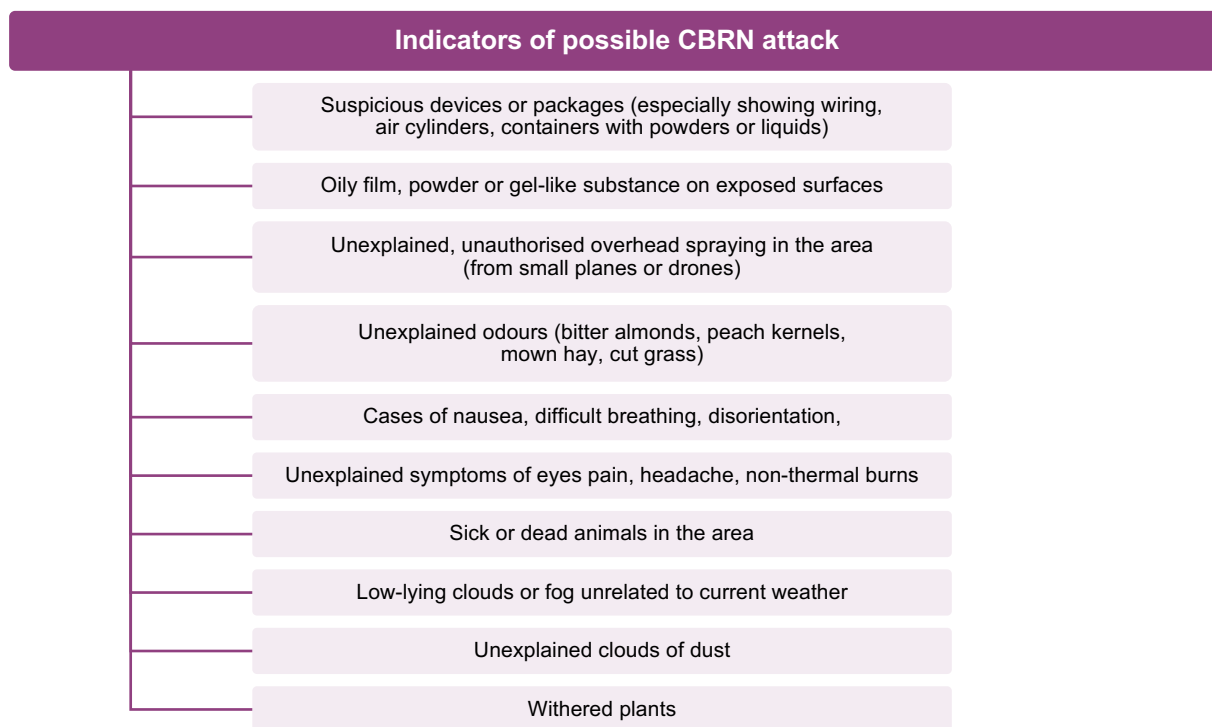
Administrator of the PW or incident manager is in charge of the situation until LEA arrives. In a situation where the explosive device has not yet been located, incident manager recommends that the PW staff should check:

- items that were not there before and were not brought by the PW staff;
- traces of displacement of room furnishings;
- changes in the external appearance of objects and the signals emitted from them (e.g. sounds of clock mechanisms, glowing electronic elements, etc.);

at public spaces, such as: corridors, staircases, lobbies, elevators, toilets, basements, attics, etc., and the closest external surroundings of the facility. If the PW staff find the presence of objects that were not there before or changes in the appearance and location of objects permanently present in the facility, it can be assumed that they may be explosive devices. It is forbidden to touch such objects. The information about it should be reported to LEA⁶.

Characteristic of CBRN threat is described in deliverable *D4.1 Introduction to CBRN threats*. As presented there the consequences of such an event depend on many factors like: toxicity of agent, way of exposure, time of exposure, actual weather conditions and many more. In general and in most cases it will be difficult to detect and identify a release of CBRN agent in an initial stage of the incident. However, there are some indicators that might be helpful in recognizing such threats (Figure 1).

Figure 1 – Possible indicators of a CBRN incident



Source: Deliverable D 4.1. Introduction to CBRN threats.

⁶ <https://www.gov.pl/attachment/a0b0c901-675f-41bc-ae53-22647d490b0c>

When the information about the incident is reported to an emergency number operator, it might be useful to specify:

- Why situation is suspicious?
- Is the place/building high or low profile?
- Are there any messages or intelligence about that suggest the incident?
- Who found it and when?
- Where is the threat?
- Who has had contact with suspicious material, where is that person now?
- What are local weather conditions?
- Is the threat inside the building or in an open space?

Each threat evokes emotions, therefore try to stay calm when talking to the emergency number operator. Be precise when communicating details. Remain on the phone until you receive a clear message that you can hang up. Be aware that the emergency number operator or rescue services dispatchers may want to reconnect you afterwards.

Do not hesitate to call the emergency number again if the situation on the scene changes before first responders appear on the scene. Updated information makes it possible to redirect already appointed units and alert new ones, if required by the situation.

2. A model example of cooperation at the action scene of the religious sites

As mentioned before there is no representative religious site. Large gatherings are organized inside the buildings (e.g. church, mosque), in the area of sanctuaries, but also at stadiums, roads (pilgrimages) and other open areas. Each religious organization has its own practice of organizing ceremonies, especially those that are highly symbolic or events that gather a large number of believers.

Different countries has its own legal system which defines responsibilities for law enforcement agencies (LEA) and rescue services. Therefore it is possible to define only some general assumptions of cooperation between the organizers of religious celebrations and the services responsible for responding to an emergency.

In the context of cooperation, good practices to support the protection of public spaces⁷ defines to appoint contact points and clarify respective roles and responsibilities on security matters at both sides – organizer, LEA and emergency services.

The organizational structure on the part of the organizer of the religious ceremony may be limited to those who are involved in the direct conduction of the ceremony or expanded to include information, technical or security services and others (Figure 2).

Figure 2 – Religious event's stakeholders



Source: own elaboration.

Priest, imam, rabbi, pastor and other leader of a ceremony and other persons (cantor, acolyte, other) are directly involved in a ceremony conduction⁸. Hence technical staff of ceremony/PW ensures proper

⁷ Good practices to support the protection of public spaces, source: <https://op.europa.eu/en/publication-detail/-/publication/998aeb09-4be6-11e9-a8ed-01aa75ed71a1/language-en>

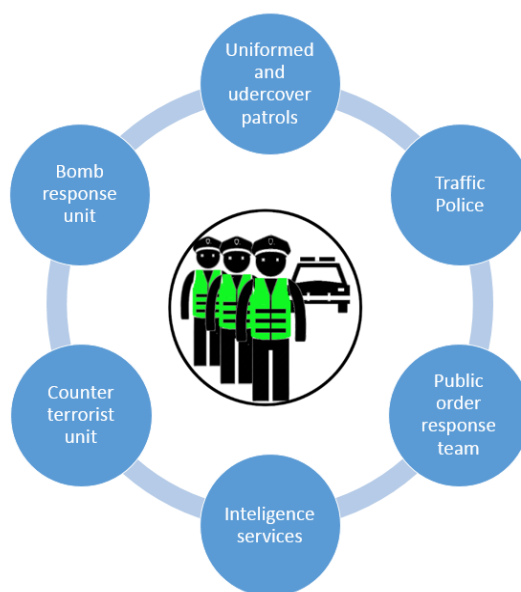
⁸ Priesthood in the religions of the world, Eds. W. Cisło, J. Różański, Instytut Dialogu Kultury i Religii, Wydział Teologiczny UKSW, Warszawa 2013

operation of all systems (sound system, lights, candles, etc.) necessary to conduct ceremony and also proper functioning of the facility (ventilation, access control, CCTV, etc.). Welcome team staff, that accept welcoming worshipers, should assist visitors and people with disabilities, provide information about facility, show the way. Security service provide parking lot and entrance security check, CCTV monitoring, securing the worshipers outside the facility e.g. during the procession. Intelligence service might be responsible for internet/media monitoring, contact with other religious communities and LEA's. Crisis management team gathers representatives of all groups involved in the celebration conduction and provide a service to carry out its activities when a threat occurs. Such a team cooperates with the LEA and emergency services that arrive at the scene.

It is highly important that an event plan is developed in a religious event preparation stage. Description of emergency procedures, roles and responsibilities should be there⁹. Regardless of the organizational structure of the religious event, it is necessary to appoint a person who is responsible for the safety and security of the assembly. Such an 'incident manager' should have been trained in emergency procedures and, for the purpose of better recognizability during an event, he/she should be dressed in a way that differs him/her from other organizer's staff (e.g. vest, hat).

Law enforcement agencies (LEAs) and emergency services are responsible for protection of people's health and life, protection of public safety and security as well as for an order and control of compliance with regulations concerning public life and public spaces (Figure 3).

Figure 3 – Law enforcement agencies possible roles in religious event



Source: own elaboration.

Until a threat occurs most of the tasks LEA's perform outside the religious event sites. The appearance of uniformed officers at religious gathering locations is usually reduced to the cases when there is a request from the organizer to LEAs forwarded. LEAs have the leading role in case of responding to terrorist incidents. Among the tasks of the LEAs, it is necessary to indicate: responding to firearms attack, sharp object attack, vehicle attack, IED- explosives, PBIED- explosives, UAVIED- drone, VBIED- explosives, CBRN:

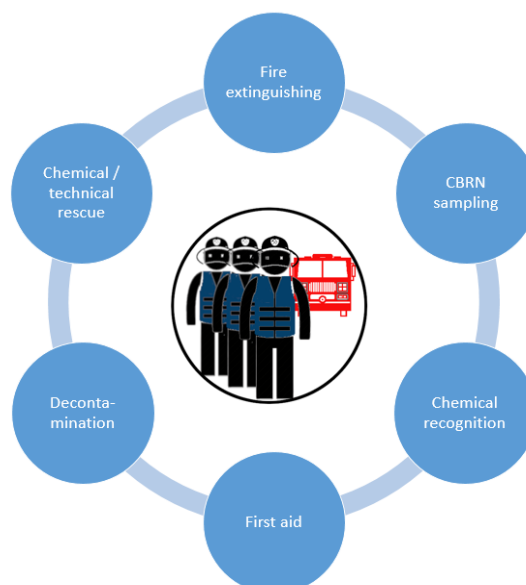
⁹ Facility or event security plan is one of Good practices identified which is the part of ProSPeReS document Set of procedures to prevent, protect, detect, respond and mitigate the result of terrorist attacks

- ensuring public safety and order in the area of operations;
- designation of a safety zone;
- protection and isolation of the endangered area;
- isolation of the endangered area;
- ensuring safety and order in road traffic (in the area of the operation area);
- organizing and informing about detours to endangered areas;
- conducting negotiations;
- the use of devices that prevent third parties from telecommunications in a specific area;
- checking the facility by the Bomb response unit to reveal the explosive device;
- neutralization of explosive materials or devices;
- activities related to the disclosure of the data of the person reporting the planting of the explosive/CBRN;
- activities related to free the hostages (and unlock the facilities);
- evacuation of people;
- psychological support.

All the activities of LEAs are carried out under command of the chief of operation.

Rescue services e.g. fire brigade are formed to react in life, health or environment threatening situations. They responding in case of fires and other threats, providing chemical (haz-mat) and technical rescue, water and diving rescue, urban search & rescue, first medical aid. As part of their activities, they conduct rescue operations related to the events with CBRN factors (**Error! Not a valid bookmark self-reference.**).

Figure 4 – Fire & rescue service possible roles in religious event



Source: own elaboration.

The presence of emergency services at the scene of the event before the hazard occurs is possible mainly in the form of first aid spots or patrols. Other forms of presence are also possible, if agreed at the preparation stage of the religious event. Temporary posts with proper resources (e.g. decontamination modules) might be established.

Rescue services in case of a terrorist attack are responsible for:

- recognizing and securing the scene of the event;
- recognizing and identifying the threat and forecasting its development;
- performing image recognition using advanced technical means (e.g. robots, drones, optoelectronic devices);
- designation and marking of threat zones;
- sampling;
- reaching and making access to endangered or injured people;
- evacuation of injured and endangered people and animals out of the threat zone;
- warning and alerting people about the threat and how to behave;
- carrying out measurements (chemical and radiological agents) using measuring instruments;
- limiting the effects of emission of hazardous materials;
- conducting initial decontamination of people, including rescuers;
- decontamination of equipment;
- providing qualified first aid;
- switching installations, devices and utilities on or off for rescue operations purposes;
- control of the emission of hazardous materials;
- relocating of dangerous goods;
- other tasks not directly connected to CBRN threats e.g. fire extinguishing, technical rescue (cutting, spreading, stabilizing structures and vehicles, etc.).

All the activities of emergency services at terrorist events are performed as supportive for LEAs.

Emergency medical service (EMS) is responsible for providing assistance to any person in a state of emergency by urgent pre-hospital treatment for people with serious illness and injuries. EMS provides transport to a hospital (road, air). In some countries e.g. Poland hospital emergency rooms are the part of EMS.

At the religious event sites before a terrorist threat occurs, EMS might provide first aid spots or patrols.

In case of a terrorist attack, EMS provides:

- triage;
- providing pre-hospital medical care;
- transport to a hospital (emergency room, trauma center);
- decontamination (at emergency room).

Diversity of potential threats at the action scene of religious sites cause that many types of LEAs and emergency services might be engaged in operation. In the preparatory phase there should be a matrix of roles and responsibilities¹⁰ agreed and explained. Even if all the LEAs and emergency services are involved, the leading role depend on the type of threat. Incident manager should provide all information to the leading agency on the scene. In case of a terrorist events, LEA has the leading role.

When the threat occurs initial information should be provided to the EU emergency number (112) or directly to LEA's liaison officer by the incident manager.

If there is no emergency services on site the organizer is responsible for leading and coordinating the response during an emergency situation. The organizer should provide clear access roads for emergency services.

Incident manager with other staff should communicate worshipers directions in order to obtain the appropriate behavior (lockdown, evacuation, other), adequate to the threat. Moreover, the staff should follow the directions in the facility management (lock/open doors, switching installations, devices and utilities on or off).

When the emergency services are present on site, the incident manager should provide necessary information including facility documentation (plans of buildings, installations, etc.). In addition the incident manager should support the response by communicating and coordinating the place of worship staff.

The whole communication of organizer's staff, especially related to safety and security issues, should be known to incident manager. In case of religious events organized in large areas, it is common to use the open channel radio transmitters for the organizers communication purposes. It is a good practice, however it is not possible to use such means of communication among emergency services.

The communication channels among emergency services and also incident manager should be established. There is common understanding and practice among LEAs and rescue services how to communicate and cooperate in such situations, however it is crucial to incorporate a religious event incident manager properly into this structure.

Means and channels of communication should be established in the preparatory phase of the event. If phone connection is an agreed way of communication between the organizer and rescue services, it is important to use a separate phone number for that purpose. In a case of an emergency, the incident manager has to contact LEAs and other emergency services immediately. That's why the communication with other staff members mustn't block the dedicated phone line.

¹⁰ Roles and responsibilities matrix contain information: Kind of threat, risk (optionally), leading service/agency, involved services/agencies, tasks.

3. Models for cooperation and notification in large scale religious events

Cooperation between the organizer of a religious event and LEA's and first responder organizations should start as soon as possible, and definitely not later than in the preparation phase to the event. The cooperation ideally should be permanent, regardless of the organization of large gathering. As it is the case then the basic level, a fundament for cooperation between PW administration and local police officer is already in place.

For the large scale religious events preparation, the cooperation usually takes place at the level of the representative of the curia and the police officer of the regional/city headquarters. The extent of LEA's involvement is expected as the preparation proceeds. Thus, it is important to appoint representatives on both sides who are responsible for communication during the preparation phase as well as during event itself.

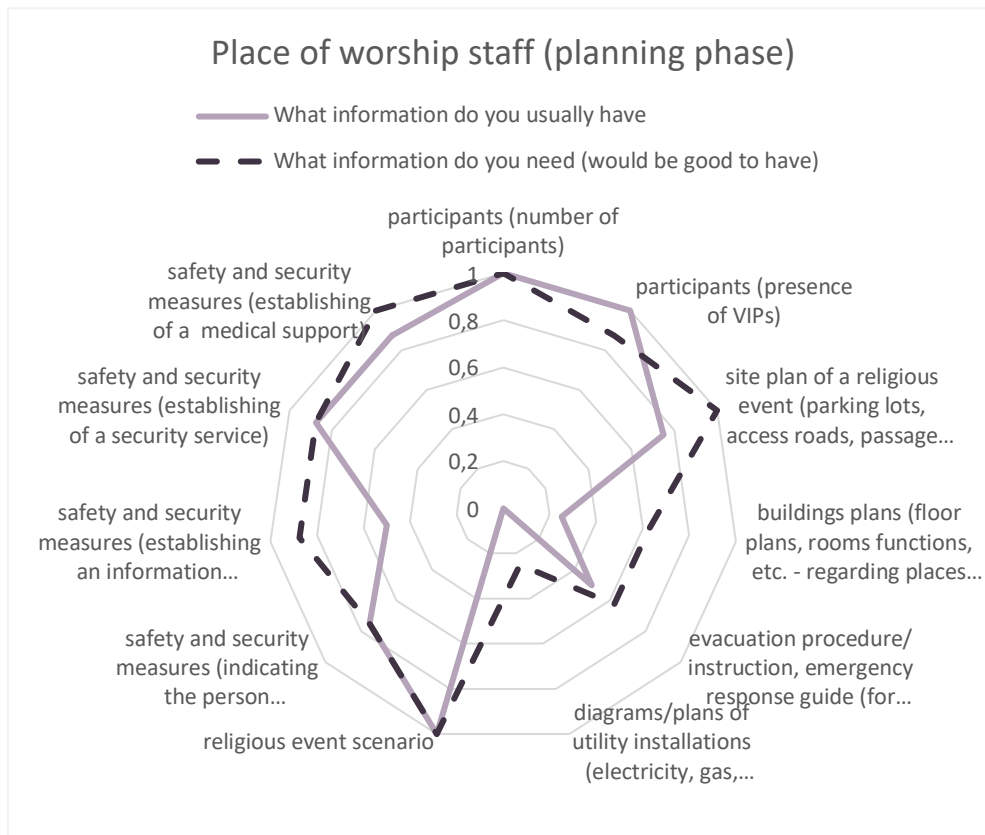
In some cases the scope of cooperation may be limited to managing traffic and ensuring safety on the access roads to the place of the religious event by LEA's officers. Deployment of patrols results from analyzes carried out by LEA's and based on information received from the organizer on the current situation.

However, in case of a terrorist attack, the organizer should follow arrangements set at the preparation stage. If no other channels had previously been established, an emergency call must be forwarded to the emergency number. Until the time LEA's representative arrives at the scene and the situation possible change, following, updating notifications must be communicated the same way. Upon arrival of a LEA's representative, notifications should directly be made to the responding unit of LEA (not through the emergency call). As the number of LEA's officers and other resources increasing, the officer in charge might change. It is important that the representative of the religious event organizer remains in close and constant contact with the designated officer at all times.

Wider cooperation from the perspective of coordination is characterized by the constant presence of a LEA liaison officer at the religious event site. This may be the case when there is agreed to involve more LEA's resources, other difficulties or major threats are foreseen *in advance* (at the stage of preparation phase). Temporary resources allocation might be created in the vicinity of the event as well. Other arrangements, such as the presence of undercover patrols, may also be used. The representative of the organizer reports directly to LEA liaison officer in the case of a terrorist attack. An internal LEA information flow among is realized on routine basis.

The scope of cooperation mirrors the spectrum of information exchange among stakeholders. In frame of A.3.5 there has been a study conducted that focuses on the aspects of information possessed and required by the entities involved in the preparation and response during a large religious gathering. The survey was addressed to representatives of the places of worship staff, law enforcement agencies and fire & rescue units. Questions related to: 1/ preparation phase of a religious event (11 categories of information were taken into account) and, 2/ initial phase of response (with 15 categories as well).

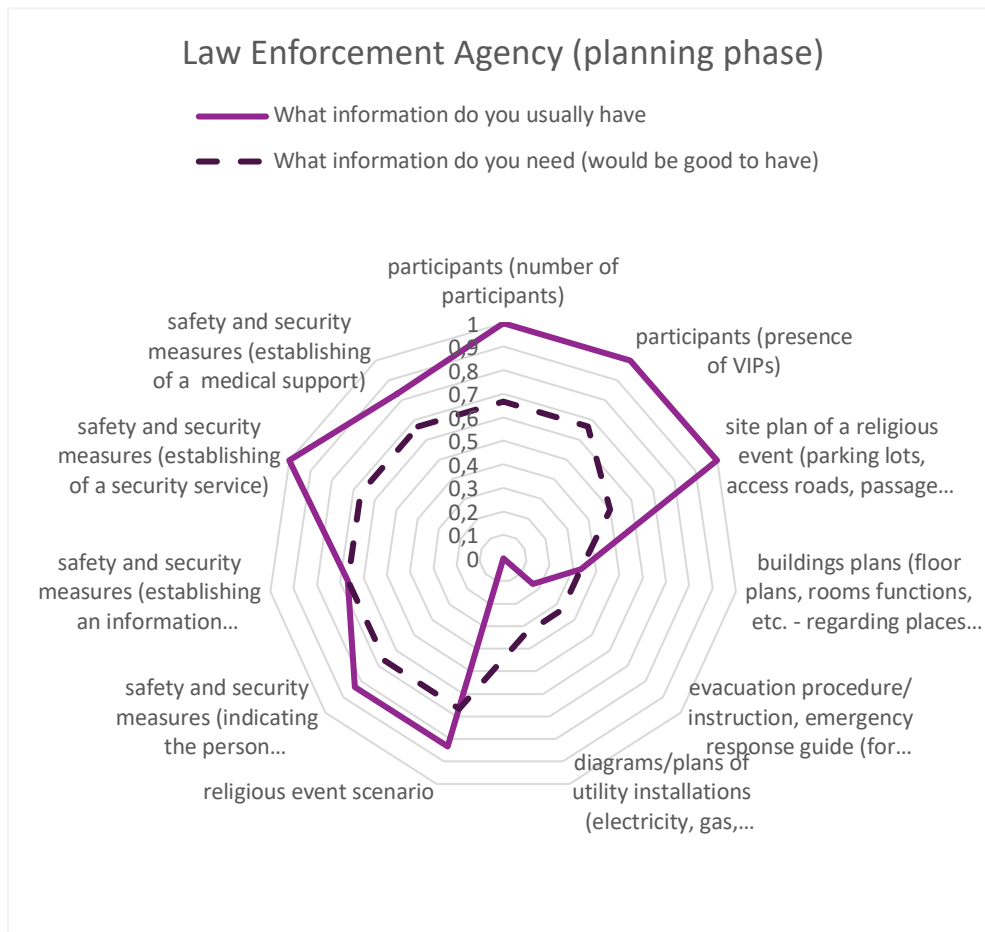
From perspective of quantitative research methodology the results of the survey are not representative due to the number of respondents (n=28), however from the perspective of an expert study they indicate information management gaps as well as potential stakeholders who might mitigate these gaps.

Figure 5 – Place of worship staff information possessed and necessary – planning phase

Source: own elaboration

As Figure 5 depicts the most noticeable differences between information that is possessed vs. required by the PW staff at planning stage. These are the ones related to:

- safety and security measures (establishing an information service/ welcome team);
- buildings plans (floor plans, rooms functions, etc. - regarding places of religious worship);
- diagrams/plans of utility installations (electricity, gas, water, heating, air conditioning, etc.).

Figure 6 – LEA information possessed and necessary – planning phase

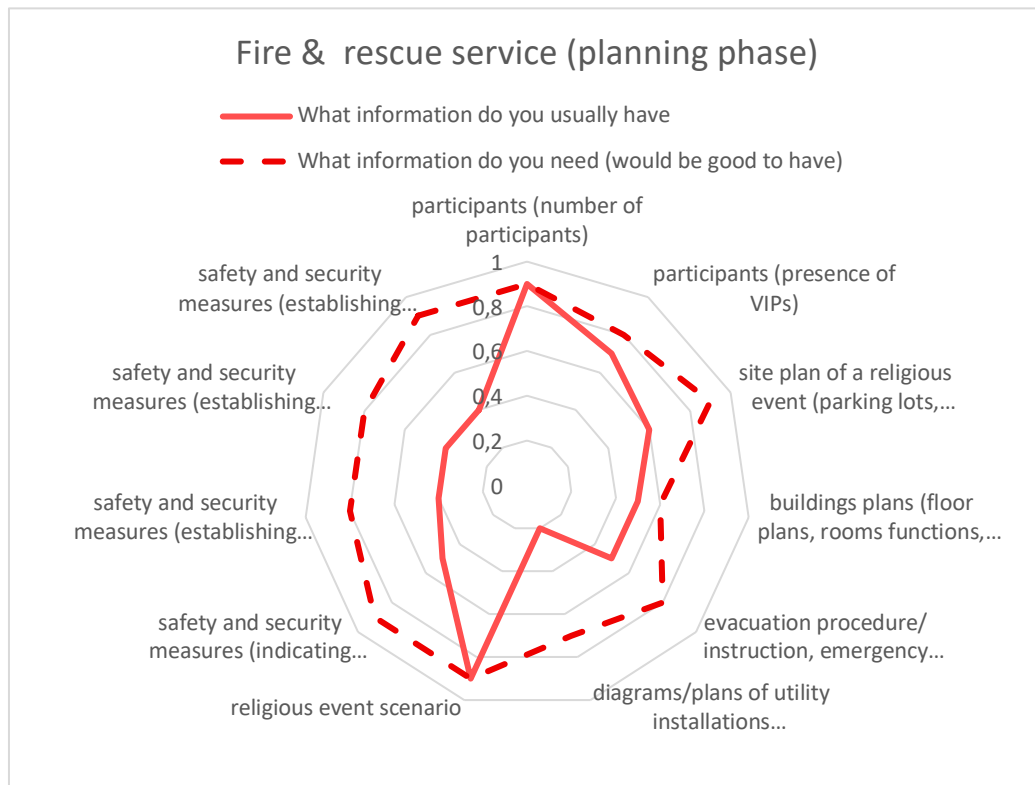
Source: own elaboration

Figure 6 shows that the two noticeable differences between information possessed and required by LEA at a planning stage are as follow:

- diagrams/plans of utility installations (electricity, gas, water, heating, air conditioning, etc.);
- evacuation procedure/ instruction, emergency response guide (for place of worship).

In other categories, the information possessed by LEA representatives exceeds their information needs what might be interpreted that for these criteria LEA is relatively satisfied with the data they usually have.

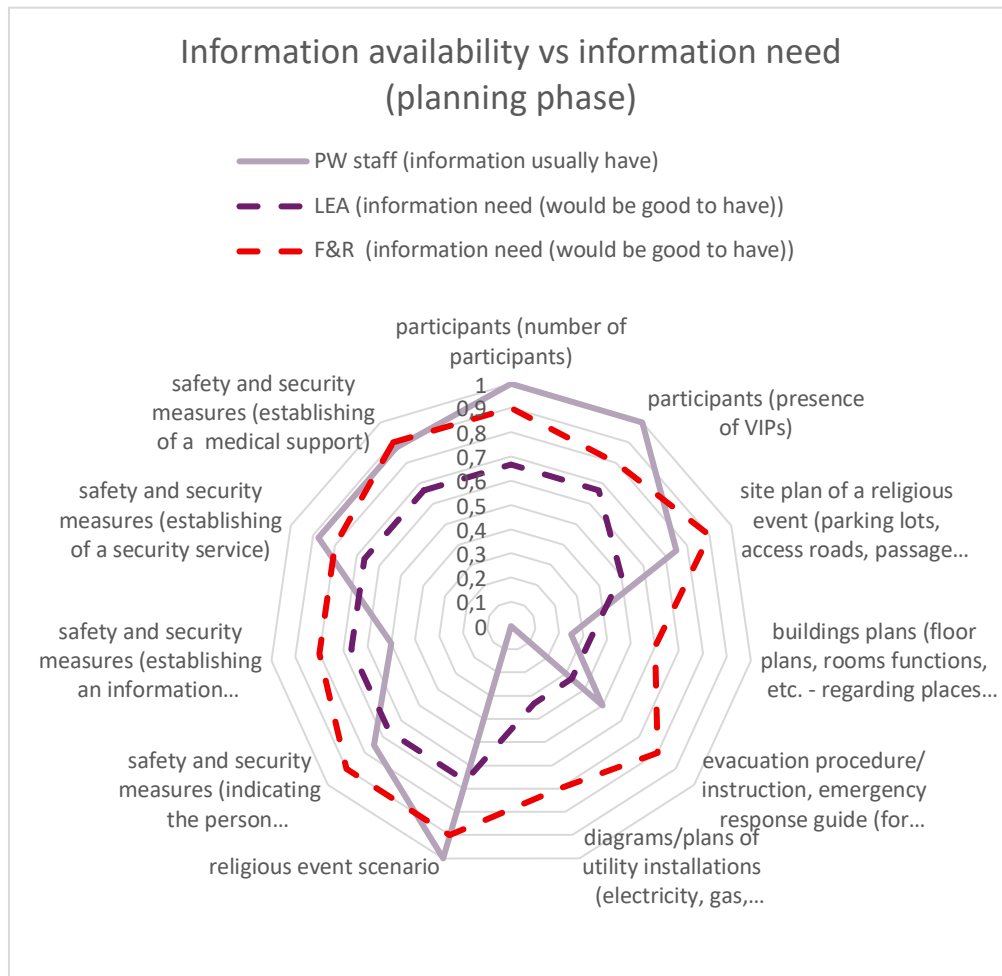
Figure 7 – Fire & rescue services information possessed and necessary – planning phase



Source: own elaboration

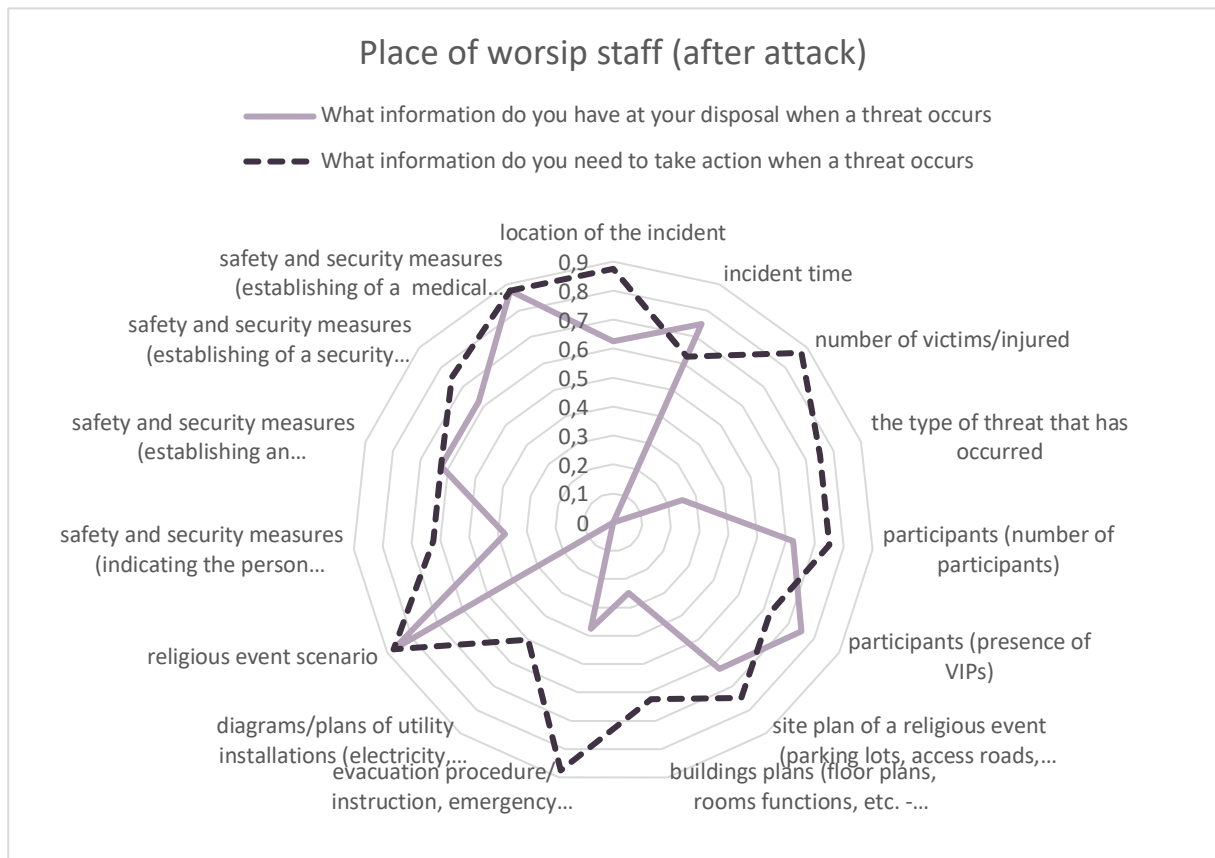
Figure 7 indicates information needs of fire and rescue (F&R) units. There is a deficit of information in most of the criteria. According to the fire and rescue respondents there are the only two categories that are sufficiently covered by the information flow at the stage of preparatory to a religious event. These are 1/ participants (number of participants) and, 2/ religious event scenario are at a sufficient level.

Figure 8 – Information possessed by place of worship staff vs information necessary by LEA and fire & rescue services – planning phase



Source: own elaboration

Figure 8 puts together the information needs of LEA and F&R with the information that is possessed by PW at the stage of preparation to a religious event. The graph depicts that there is a number of information gaps of the two services that might be covered by an appropriate communication flow from PW to LEA and F&R since PW is in possession of the information needed by public services. The potential information categories that are expected to be improved in communication protocols are as follow: participants (number of participants), participants (presence of VIPs), religious event scenario and safety and security measures (establishing of a security service).

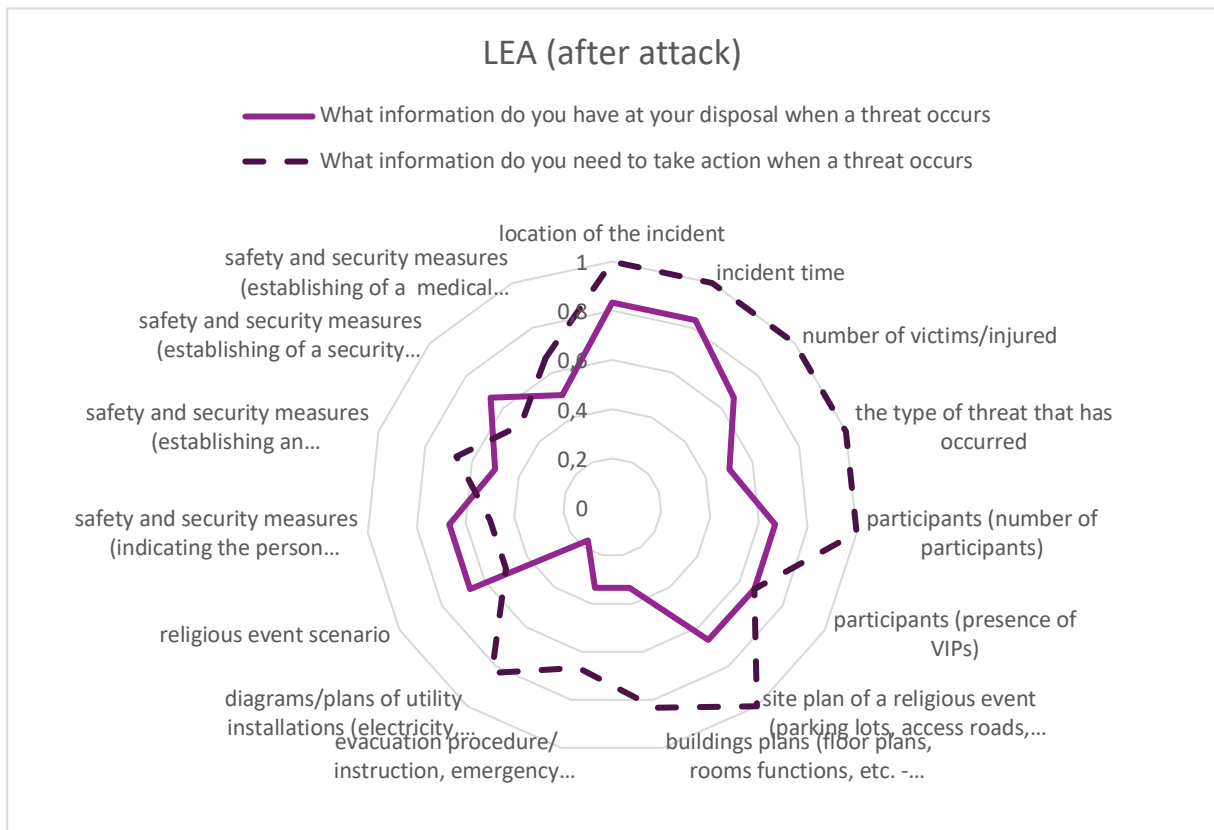
Figure 9 – Place of worship staff information possessed and necessary – initial response phase

Source: own elaboration

Figure 9 presents a relation between PW's information needs that might appear right after an attack vs. the information the PW representatives are usually in possession at the given stage. Once the threat materializes (after attack), the biggest difference between information that is possessed vs. required by the PW staff appears to be as follow:

- number of victims/injured;
- the type of threat that has occurred;
- evacuation procedure/ instruction, emergency response guide (for place of worship).

These information categories seem to be in need of coverage by relevant communication protocols with other stakeholders at the stage of the initial response.

Figure 10 – LEA information possessed and necessary – initial response phase

Source: own elaboration

As shown at Figure 10 for initial response to a terrorist attack, LEA representatives seem to be short of most of the surveyed information categories. However, there are some exception in which LEA is satisfied with the information they have. They are as follow:

- participants (presence of VIPs);
- religious event scenario;
- safety and security measures (indicating the person responsible for cooperation with other entities);
- safety and security measures (establishing of a security service).

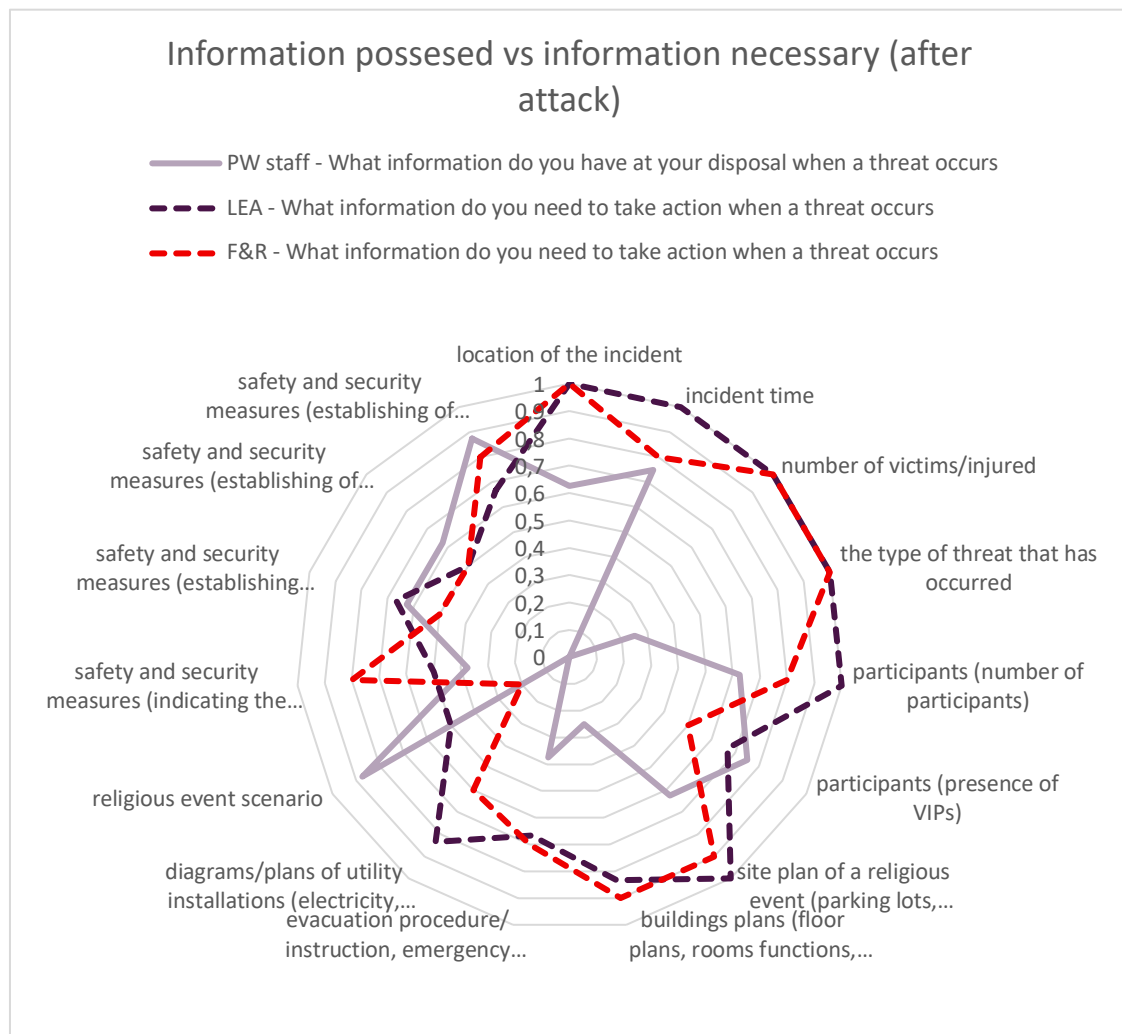
Figure 11 – Fire & rescue information possessed and necessary – initial response phase

Source: own elaboration

Figure 11 shows that in the initial response phase, F&R relatively needs more information than actually possess (similar to LEA). Nevertheless, information categories that are covered at the initial response are as follow:

- location of the incident;
- incident time;
- participants (presence of VIPs);
- religious event scenario.

Figure 12 – Information possessed by place of worship staff vs information necessary by LEA and fire & rescue services – initial response phase



Source: own elaboration

Figure 12 presents information gaps of LEA and F&R at the initial response to a terrorist attack that might be covered by relevant communication protocols with PW. Basically, PW is in a position to deliver a given information to LEA and/or F&R, since PW has this particular information (as shown on the figure). However, to do so there are to be proper communication protocols introduced into the cooperation practices. The following information categories possessed by PW might be of support for LEA and/or F&R:

- participants (presence of VIPs);
- religious event scenario;
- safety and security measures (establishing of a security service);
- safety and security measures (establishing of a medical support).



prosperes.eu



This project is funded by the European Union's
Internal Security Fund – Police under Grant
Agreement No. 101034230 – ProSPeReS



How to organize Vulnerability Assessment? (VAT Lite)

Appendix 4

of GUIDEBOOK on security measures
for religious sites & communities



This project is funded by the European Union's
Internal Security Fund – Police under Grant
Agreement No. 101034230 – ProSPeReS

prosperes.eu



Please scan the QR code
to get the access to reading materials.

Preamble

Religious sites are considered to be especially vulnerable to attacks due to their accessibility and the fact that there are usually limited security measures applied.

The ProSPeReS project is aimed at increasing the level of protection in places of worship by keeping the balance between security measures and preservation of the open nature of Places of Worship.

“Better education is better prevention, protection and response to various types of terrorist threats and incidents that may occur in religious places, including attacks with chemical biological and radiological materials.”

“We are all actors in our own safety and that of others.”

WARNING

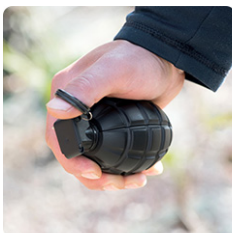
This leaflet is not intended to replace the regulations in force. Its purpose is to provide practical advice. It creates no new legal obligations in the field of safety, nor the means implemented to deal with acts aimed at harming people.

Disclaimer

Please note that the ProSPeReS Vulnerability Assessment Tool Lite Version (VAT Lite) should not be used for major religious events. In this case, risk assessment professionals should carry out an official risk assessment.

Depending on the results, the users can also refer to the guidebooks with recommendations for security measures and actions produced by ProSPeReS, available at: www.prosperes.eu

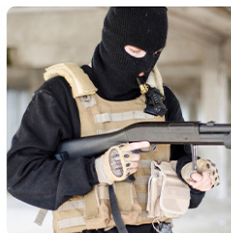
**Explosives
attack**



**Knife or sharp
object attack**



**Firearms
attack**



**Vehicle
attack**



**CBRN
attack**



VAT Lite – guidelines

- 1 **Print an online MAP** (e.g., google maps) or a site plan (A0 format works best with the provided stickers but other formats work as well) depicting the structures at your Place of Worship (PW) and its surroundings up to main access roads (see example on record template A). Next, print the stickers on page 6 of this document (not recommended if map is printed on A3 or smaller).
- 2 **Divide the PW into three (3) zones**, using a permanent marker, to indicate 1) the building and its interior, 2) the immediate exterior and 3) the surrounding area (See record template A).
- 3 **Place the most relevant threat type stickers** (see legend for stickers) for each zone, or write types of threats on sticky notes and place them on the locations within the map where these threats might or have occurred. Try to place the threats on areas within the zone that usually have high concentration of people.
- 4 **Fill out record template B, the main site information and the checklist** based on the EU Quick Guide for the protection of Places of Worship.
- 5 **Proceed with Risk Analysis by filling out record template C**, using the risk matrix.
- 6 **Finish the VAT Lite** by filling out the risk level table per phase in record template D.

Example:

In order to assess the level of a religious site's protection, the site's operator decides to conduct a quick vulnerability assessment. This will allow the operator to identify whether or not, the site is protected (at least at a basic level) against threats such as vehicle ramming attacks. Following the previous step of the VAT Lite template, the site's operator will discuss with other competent staff members who are familiar with the operations, activities and facilities of the site, the consequences and likelihood of hypothetical attacks against the site.

At first, they will discuss the consequences of a speeding truck been driven into the site's courtyard where worshippers are gathered. If such an attack would occur and more than 100 people are present during the incident, casualties could be quite high. Therefore, in table 5, next to "vehicle attack" they will write down "HIGH" consequences. They will then consider the likelihood of the attack happening by considering important relevant risk factors (e.g., expression of hate against your religious community or similar incidents against other religious sites). In this example, there have been no signs of suspicious behavior, but they are aware of some tensions. They consider the likelihood of an attack to be "MEDIUM". The final step is to then multiply the Consequence and Likelihood using the provided Risk Matrix, in order to get a final Risk Score for the discussed attack. Looking at the Risk Matrix HIGH consequences x MEDIUM likelihood = HIGH risk level.

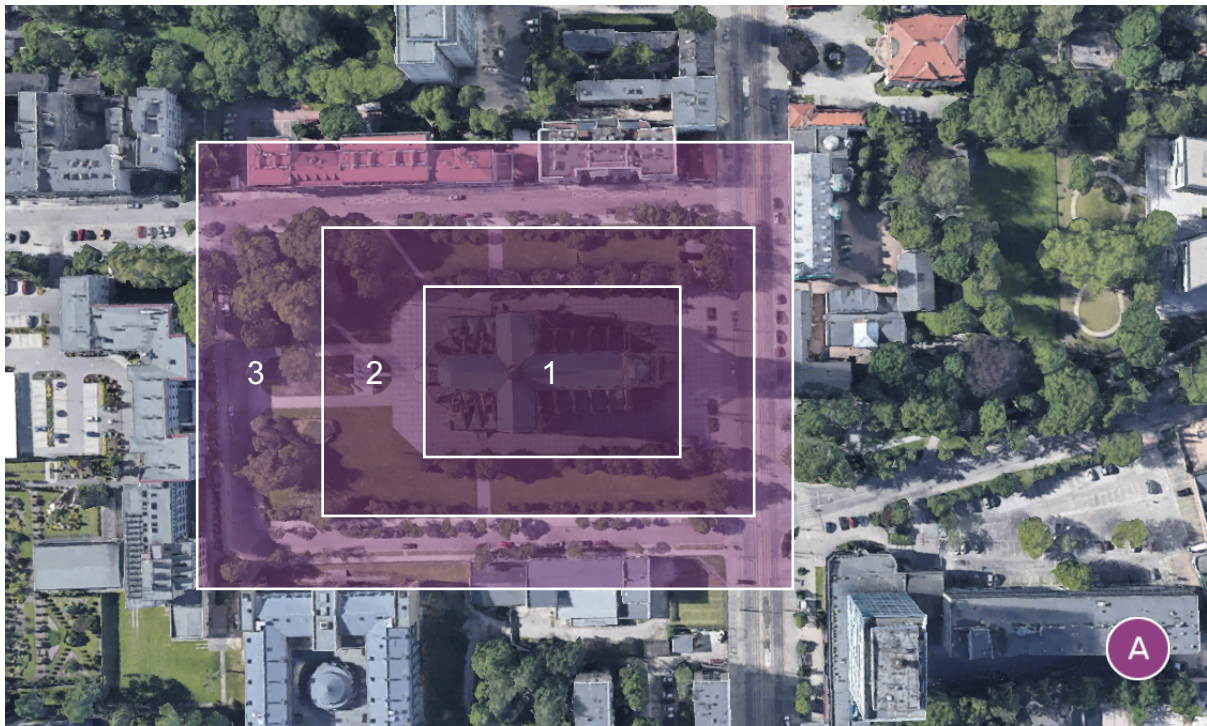
		Likelihood (Probability)				
		Very Low	Low	Medium	High	Very High
Consequences	Very Low	Very Low	Very Low	Low	Low	Medium
	Low	Very Low	Low	Medium	Medium	High
	Medium	Low	Medium	Medium	High	High
	High	Low	Medium	High	High	Very High
	Very High	Medium	High	High	Very High	Very High

VAT Lite – Record Template A

2

Print out a map of your PW of interest. Divide the PW into three (3) zones using a pen or markers. To indicate 1) the building and its interior, 2) the immediate exterior and 3) the surrounding area.

As seen in the examples A & B:



Actual example of VAT Lite Workshop

- Zone 1
INTERIOR (PW inside)
- Zone 2
EXTERIOR (PW immediate outside)
- Zone 3
SURROUNDINGS (parking lot, terrain surrounding PW)



VAT Lite – Record Template B



MAIN SITE INFORMATION	
Main site name / address	
Description, date & time of activity	
Whom to call in case of emergency	
Date of assessment	

Checklist		Yes	No	N/A
ZONE 1	Are there access control measures for the visitors in place (e.g. x-ray machines, metal detector gates etc.)? Difficulty: 2			
	Are the main door and windows or main access point locked during closing hours? If the place of worship is open 24/7 please answer "NO" Difficulty: 1			
	Are there locking mechanisms, bars, or other materials (e.g. impact resistant window films or reinforced glass) installed on the windows to prevent break-ins or dangerous items thrown into the building? Difficulty: 1			
	Do you have a CCTV system installed for monitoring the areas within the building where people gather, or valuable items are kept? Difficulty: 2			
	Is there a security system with a silent alarm that is connected to the police or a private security provider? Difficulty: 2			
	Do you have a fire alarm in place? Difficulty: 2			
	Do you have signage in front of the place of worship indicating the existence of security measures inside the facility (e.g. CCTV or security officers warning)? Difficulty: 1			
	Does the main building have emergency exits? Difficulty: 3			
	Does your place of worship have a procedure for the staff to monitor parcels or items received at the place of worship? If you don't receive parcels at the place of worship please don't answer this question. Difficulty: 3			
Do you have measures or a policy for unattended suspicious items at you place of worship? Difficulty: 2				
ZONE 2	Is the main gate locked during closing hours? If there is not a gate in place answer "NO". Difficulty: 1			
	Are there measures in place (e.g. Bollards, street furniture) preventing (speeding) cars from entering the area outside the main building where people gather? Difficulty: 3			
	If there is a parking lot at your place of worship, does it have access control measures for the cars entering it? If there is not a parking lot in this zone, don't answer this question Difficulty: 2			
	If there is a parking lot at your place of worship, does it have sufficient lighting? If there is not a parking lot in this zone, don't answer this question Difficulty: 2			
	If you have a CCTV (Closed Circuit Television; camera surveillance) capable of monitoring areas the areas outside the building where people gather? If you don't have a CCTV system in place don't answer this question Difficulty: 2			
	Do you have sufficient lighting in the area around the main building to eliminate dark areas and hiding spots? Difficulty: 2			
ZONE 3	If there is a parking lot adjacent your place of worship, does it have access control measures for the cars entering it? If there is not a parking lot in this zone, don't answer this question Difficulty: 3			
	If there is a parking lot adjacent your place of worship, does it have sufficient lighting? If there is not a parking lot in this zone, don't answer this question Difficulty: 3			
	Do you have sufficient lighting in the area to enhance monitoring and eliminate dark secluded areas? Difficulty: 1			
	Are there usually police officers patrolling the area around the site? Difficulty: 3			
	Are there any streets around the site that allow speeding vehicles to have direct access to the premises of your place of worship / areas of people gathering? Difficulty: 2			
	Is there usually a high number of parked vehicles around the place of worship (e.g. for bomb placement) Difficulty: 1			
GENERAL QUESTIONS	Are the staff members supporting the activities of the place of worship trained to carry out the emergency procedures? Difficulty: 3			
	Have you in the past conducted any type of emergency response trials to see how your facility staff will perform in a crisis situation? Difficulty: 3			
	Are there any designated evacuation routes? Difficulty: 2			
	Are the evacuation routes clear and unobstructed to facilitate an emergency evacuation / invacuation? Difficulty: 1			

POINTS:

--	--	--

* The scores of the questions reflect the implementation complexity/difficulty of possible security measures. Count the no's.
 ** The questions were randomly filled out as an example.

VERY BASIC RISK INDICATORS

For questions with difficulty 1 (low)
 For questions with difficulty 2 (medium)
 For questions with difficulty 3 (high)

ACTION

Continue by filling out the VAT Lite template and think of possible solutions to implement by yourself.
 Fill out VAT Lite and think of solutions. You may need to contact technicians, technical solution providers or urban designers in order to adopt some required solutions
 It is recommended to contact your local Law Enforcement Agency, First responders or a private security solutions provider, to carry out a thorough risk assessment and assist you with the adoption of appropriate solutions.

VAT Lite – Record Template C



Fill out 1 table per zone!

Consequences – Think of casualties, damage or injuries, based on the number of visitors at the PW, based on your experience and knowledge.

Likelihood – How likely will this threat occur in this zone, based on current security measures, past incidents and your knowledge / experience?

	Scenario per threat type	Consequence (very low, low, medium or high, very high)	Why?	Likelihood (very low, low, medium or high, very high)	Why?	C x L (risk level)
ZONE 1	Knife or sharp object attack					
	Firearms attack					
	Vehicle attack					
	Explosives attack (e.g. thrown inside building or installed in a car)					
	CBR attack					
ZONE 2	Knife or sharp object attack					
	Firearms attack					
	Vehicle attack					
	Explosives attack (e.g. thrown inside building or installed in a car)					
	CBR attack					
ZONE 3	Knife or sharp object attack					
	Firearms attack					
	Vehicle attack					
	Explosives attack (e.g. thrown inside building or installed in a car)					
	CBR attack					

Risk Matrix (Risk Analysis)

Please scan the QR code to get the access to reading materials.



		Likelihood (Probability)				
		Very Low	Low	Medium	High	Very High
Consequences	Very Low	Very Low	Very Low	Low	Low	Medium
	Low	Very Low	Low	Medium	Medium	High
	Medium	Low	Medium	Medium	High	High
	High	Low	Medium	High	High	Very High
	Very High	Medium	High	High	Very High	Very High

VAT Lite – Record Template D



Overall risk level

(Risk evaluation)

Risk level: This corresponds to the C x L column in the previous table (Template C).

Action: Go back to Template B. Check which **NOs** you can turn into **YES**
+ check for dangerous items before mass starts, when entering the PW.

		THREAT TYPE				
		Knife or sharp object attack	Firearms attack	Vehicle attack	CBRN attack	Explosives attack
ZONE 1	Risk level					
	What actions are required?					
	Difficulty level for action					

ZONE 2	Risk level					
	What actions are required?					
	Difficulty level for action					

ZONE 3	Risk level					
	What actions are required?					
	Difficulty level for action					

VAT Lite – Legend for stickers

Print out the stickers on the next page to put them on the printed map of your PW
(Step 3, Record Template A)



Firearms Attack (FAA)

e.g. small calibre pistol or semi/ fully automatic rifle AK-47



Vehicle Ramming Attack

e.g. vehicle driven into large crowds



Explosives

e.g. carried / dumped / concealed in objects or goods



Bladed Weapon Attack (BWA)

e.g. knives, machetes, other sharp or blunt objects



CBR released or dispersed with explosives

e.g. threat object concealed in goods or carried items-ex. teargas canister (chemical), concealed in goods or carried items (biological), threat object concealed in goods or carried items (radiological)



Feelings of insecurity





prosperes.eu



This project is funded by the European Union's
Internal Security Fund – Police under Grant
Agreement No. 101034230 – ProSPeReS

THE **TEN** RULES



- 1** Conduct a risk analysis & vulnerability assessment for the places of worship.
- 2** When planning a new building/facility location, consider security measures from the Security-by-Design concept.
- 3** Include the issue of security awareness in the organisational culture of your community, including its provision at the management and strategic levels.
- 4** Ensure proper maintenance of the facility – order, lighting, free spaces, escape routes
- 5** Considering the open nature of places of worship, monitor the available space and apply access control for selected, non-public spaces.
- 6** Install appropriate technical security measures (locks, video surveillance, motion sensors, lighting)
- 7** Include the issue of security awareness in the organisational culture of your community, including its provision at the management and strategic levels.
- 8** When recruiting employees or contracting services, check personal data and references.
- 9** Consider how best to secure places of worship's data, including information systems.
- 10** Plan proper behaviors/procedures in a crisis situation.

SECURITY ROUTINE CHECKLIST

If applicable check:	Daily			Weekly			Monthly			Remarks
	date:			date:			date:			
	YES	NO		YES	NO		YES	NO		
External premises										
the outer fence for signs of forced entry	x									
in the morning if any objects have been thrown over the fence into the premises	x									
the correct operation of the security systems installed on the external fence				x						
that the cameras of the CCTV system do not need to be adjusted and are not obscured (e.g. by vegetation)							x			
the outside area for any suspicious vehicles	x									
the outside area for any left objects	x									
proper operation of the installed anti-terrorist protection at the entry points				x						
rubbish bins for any suspicious objects	x									
for disturbed soil in unplanned areas	x									
the correct operation of the lighting, especially in sensitive areas				x						
the correct functioning of the installed security systems				x						
objects left behind - in places not intended for them	x									
air intake protection							x			
the objects on the property for signs of tampering	x									
the patency of escape routes				x						
the air intake protection							x			
assembly points to see if it is possible and safe to evacuate to that location				x						
the emergency services have information on the location of these points										annually
if access roads are properly maintained for quick and efficient movement of emergency services				x						
Access points										
every morning the door for signs of damage, tampering, opening	x									
every morning the windows for damage, tampering opening, or breaking	x									
correct functioning of intercom and door-opening mechanisms				x						
correct operation of access control				x						
before the closing check for the appropriate closing of each access point (doors, windows, roof, basement, etc.)	x									
Inside										
before closing, check for left items between the benches and within the facility	x									
While opening check for left items between the benches and within the facility	x									
every time you leave the premises arm the alarm system	x									
before closing empty the waste bins before leaving the facility	x									
if the security room is properly secured against unauthorized access				x						
Additionally check:										
mail and emails for threat information	x									
media information regarding safety	x									
location and completion of emergency equipment							x			
the operation of the silent alarm or warning system							x			
if the security and safety documentation is up to date							x			
the national terrorist threat level				x						
make sure the CCTV system and recorders are working	x									
check the operation of the panic button and signal operation with the security company							x			

