Title:	Document Version:
D4.3 Security policy specification Version 1	1.0

Project Number:	Project Acronym:	Project Title:
H2020-740466	LETSCROWD	Law Enforcement agencies human factor methods and Toolkit for the Security and protection of CROWDs in mass gatherings

Contractual Delivery Date:	Actual Delivery Date:	Deliverable Type*-Security*:
M10	M11	R-PU

*Type: P: Prototype; R: Report; D: Demonstrator; O: Other.

**Security Class: PU: Public; PP: Restricted to other programme participants (including the Commission); RE: Restricted to a group defined by the consortium (including the Commission); CO: Confidential, only for members of the consortium (including the Commission).

Responsible:	Organisation:	Contributing WP:
Pedro Miguel De Brito Esteves Grilo	PSP	WP4

Authors (organisation):

Pedro Miguel De Brito Esteves Grilo (PSP)

Alejandro Ruiz (ETRA)

Santiago Cáceres (ETRA)

Abstract:

This deliverable defines decision making and police intelligence key aspects to set guidelines for policy making and specification, as a guide and help for the implementation of LETSCROWD's Policy Making Toolkit.

Keywords:

Security, policy, intelpol, guidelines, police

Revision History

Revision	Date	Description	Author (Organisation)
V0.1	21.02.2018	First version, only text	Pedro De Brito (PSP)
V0.2	27.02.2018	Converted into deliverable	Alejandro Ruiz (ETRA)
V0.3	27.02.2018	Restructuration	Santiago Cáceres (ETRA)
V0.4	27.02.2018	Introduction and conclusions	Alejandro Ruiz (ETRA)
V1.0	14.03.2018	Final version	Alejandro Ruiz (ETRA)

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement № 740466.

More information available at https://letscrowd.eu

Copyright Statement

Index

LIST OF FIGURES

LIST OF TABLES

LIST OF CHECKLISTS

1 Introduction

1.1 PURPOSE OF THE DOCUMENT

This deliverable defines decision making and police intelligence key aspects to set guidelines for policy making and specification, as a guide and help for the implementation of LETSCROWD's Policy Making Toolkit.

The purpose of the deliverable is to scope down the context, defining Mass Gathering and methodologies, to then specify guidelines for Security Policy Specification.

1.2 SCOPE OF THE DOCUMENT

This deliverable is version 1 of a total of 2 versions for Security Policy Specification.

The first version scope references PSP and their methodologies for decision making, planning and risk calculation of an event, and what they consider the key points for security policy specification guidelines.

1.3 STRUCTURE OF THE DOCUMENT

The first section of the deliverable defines Mass Gathering to scope the boundaries of the context. Then it defines how LEA's build a decision, plan the pre-event and execution phases of the event and calculates risks to prevent and mitigate incidents.

Once definitions are clear, a section with current tools describes how PSP addresses the complex problem of deciding and planning an event using INTELPOL.

Once the scope is set, a list of guidelines for security policy specification forms next section. It describes the key aspects and perspectives of an event, and what has to be taken in account using checklists for a perfect planning and decision taking.

The conclusions describes a better approach of the tool and what the information will be used for.

2 Definitions

2.1 MASS GATHERING

The definition of Major Event gave by EU-SEC Project is: “a foreseeable event that should have at least one of the following characteristics[1]:

- Historical, political significance or popularity;
- Large media coverage and/or international media attendance;
- Participation of citizens from different countries and/or possible target group;
- Participation of VIPs and/or dignitaries;
- High numbers of people and poses the potential of threats and therefore may require international cooperation and assistance.”

The relevance of the definition of a major event in the present context is obvious when we consider that a mass gathering of people with the same purpose always translates into a major event according with the above definition, and it is also certain that the spontaneous generation of a mass gathering of people does not admit any preparation and therefore make it impossible to delineate a dedicated evidence based policy.

2.2 DECISION MAKING AND INTELLIGENCE

Deciding involves making choices against a range of options and whose objectives and outcomes lie in the future, so that the decision-maker must take into account the variables that can influence the decision-making context, the opportunities and threats, as well as assess the potential consequences of existing options, with the purpose of safeguarding the fulfilment of a given mission.

Knowledge and direction to decision makers anticipate or perceive threats and systemic adversities, allowing timely adaptation of the actions to be developed.

The main objective of Intelligence is consequently the excellence of the knowledge of what is happening and the corresponding prospective capacity.

In fact, most decisions inherently have a certain degree of uncertainty as they relate to future events whose predictability is not always easy to measure, but sometimes there are situations where sufficient information is available to predict the probability of a given future event. That is, there are "uncertainty" and "risk" contexts, whose main difference lies essentially in the fact that risk factors for randomness are known and in uncertainty the rule is ignorance.

2.2.1 Police Decision Process

The "Police Decision Process" is defined as the analytical process adopted by the commander / decision-maker and his / her staff to trigger the sequence of actions / steps from the reception or establishment of the Mission until the decision taken by the Mission in a logical and enlightened manner allowing to decide on the operations in progress, ensure the correct use of available resources and plan and decide on future actions.

It should be noted that Public Order in Mass Gathering Events are a particular challenge, both for the multiple ballots to which they are subject and for their complexity to manage with the responsibility of the police

[1] EU-SEC is an initiative that UNICRI has launched in 2004 in partnership with EUROPOL and ten Member States of the European Union: Austria, Finland, France, Germany, Ireland, Italy, Portugal, Spain, the Netherlands and the United Kingdom. Funded by the European Commission, the EU-SEC Project aimed to co-ordinates national research programs on security of major EU events in Europe.

decision maker, namely: guarantee the exercise of fundamental rights; manage proportionality and adequacy of police intervention; assess risks; decide on preventive interventions.

In this type of operation, there is usually an intense psychological burden on police decision-makers, considering that the consequences of something going wrong can overflow the technical level and have repercussions at the highest level.

Thus, in situations of maintenance or restoration of public order, police responses, together with the need to comply with legal requirements, must also consider that it is preferable to prevent rather than react; preferable to negotiate rather than repress; respect of the principle of minimum intervention, in the event of the need to use coercive means.

In this way, the modalities of police action to be considered by the police decision-maker must be, in addition to being appropriate, feasible and acceptable, also flexible to face contingencies and unforeseen developments, avoiding partial or total failure of the police operation, through appropriate and timely reorientation of available resources, with reference to the pursuit of the public interest.

The police decision maker should not make the planning based on the course of events considered most likely, especially in contexts where significant potential impacts may occur. Instead, planning must follow a contingency logic, supported by the risk management process, and where it is crucial to elaborate "Scenarios", which allow to define, ponder and validate a set of decision-making options, confronting them with future situations considered plausible the scenarios are simulations of potential "future", as a consequence of which contingency plans are defined, noting that: Planning that considers this information will allow the policing commander an excellent tool to support decision-making. It will reveal mainly the various options available to deal with any problems that may arise at any given moment and their potential consequences.

2.2.2 Risk Calculation

Risk can be defined as the probability of a given threat exploiting a potential vulnerability of the system resulting in a certain impact on an asset critical to the mission and objectives of an entity, institution or nation in a given space and time.

Given the multiplicity of threats, assets to be protected and constraints arising from limited resources, risk management is paramount to prioritize assets, according to their criticality and vulnerabilities, the potential for threats and the hypothetical impact of materialization of a hostile action.

Social attitudes toward risk are becoming by and of themselves an important element of risk issues. Risks increasingly need to be managed in a way that is commensurate with societal views and perceptions. This entails a better understanding and evaluation of risk perception, and establishing two-way communication channels between risk managers and stakeholders.

The implications of each of these critical issues for the various elements of the risk management cycle are explored in the following chapters of the report.

2.2.3 Planning

Planning embodies and reflects a given decision-making process and materializes in the elaboration of a plan. The result of the planning is a plan or order of operations that assigns tasks to the subordinates, which contains necessary coordination measures to synchronize the operation, to guide the preparation of activities, to distribute resources and to establish the time band and the conditions for its execution.

The Operation Order includes, among other things, the "Concept of Operation", which must express, in a clear and concise manner, in line with the upper echelon, the commander's intention as to where, when, and how, reflecting the commander's intention and the risk he is willing to take.

In the same sense, the contingency logic of decision, within the scope of the risk management process, is based on the generation of scenarios relevant to the decision maker according to the probability of success of the threats in question and their potential impacts. Its formulation is based either on the projection of the past (known history) or on the management of uncertainty in the future.

Scenarios are considered useful both in the planning phase and during the execution of operations related with mass gathering events, since they contribute to a greater sensitivity of the police decision-maker, allowing him / her to perceive / recognize, in due time, the "signs" of possible changes emerging in the environment of operations and expedite the contingent action, minimizing the chances of being surprised, thus ensuring the best possible conditions for the fulfilment of the mission entrusted to it.

In fact, the existence of mass gathering events is likely to demand an extraordinary response, designed and delivered through a management configuration that will, most often on the basis of available intelligence and information and working within quantifiable constraints and available capacity, develop a plan or set of complementary plans to protect life, property at both the event itself and within the community beyond, with contingencies prepared to counter emerging threats and respond when unexpected situations arise.

3 State of the art: Existing tools and methodologies

3.1 POLICE INTELLIGENCE TOOL (INTELPOL)

At National Portuguese Police, grounded on the experience of many years dealing with mass gatherings, one of the most relevant instruments used to spot evidence based indicators that would help decision-makers is the police intelligence (INTELPOL).

Other examples

Ertzaintza (Police of the Basque Country) has a Multilevel Intelligence structure (Local, Territorial and Central) and in relation to prevention, mitigation and investigation in a context of major events, it offers services and intelligence products to the commanders of the units and public security services.

The coordination between agencies, the extraction, transformation and loading of intelligence data and information and their integration become a challenge that is worth overcoming.

Ertzainta state of the art will be further explained in next version of Security Policy Specification

3.1.1 Definition

INTELPOL is defined as the set of structures and activities whose objective is the production and dissemination of value-added knowledge, relative to the risks involved in missions and police activities, with the aim of contributing to the reduction of surprise and the uncertainty inherent in decision-making, and the efficiency, effectiveness, police proactivity and resilience.

The INTELPOL should provide:

- The identification of threats in terms of their potential to cause harm, including for instance threats arising from acts of hooliganism, terrorism or other crimes.
- The identification of vulnerabilities in terms of weaknesses in a defence system. Such assessments would include an evaluation of all protective and precautionary measures taken.
- The identification of risks through the process of evaluating threats and vulnerabilities. Risk assessment can be used to test plans for crisis-consequence management by developing multiple harm impact scenarios.2
-

3.1.2 Functions for decision making and intelligence

As it turns out, one of the primary functions INTELPOL within the framework of the decision-making process is to avoid surprise from the action of a given antagonist or the adverse change in the context in which a decision is made.

3.1.2.1 Police decission makingDecision Process

INTELPOL is relevant in the context of the decision, especially in its prospective aspect. This is based on the ability to foresee possibilities for plausible future events, analysing their possible implications, based on available facts and technical evidence and exploring the potential developmental directions of a given situation, providing

[2] IPO Security Planning Model

3.1.2.2 Risk Calculation

In the scope of the police decision, the management of security risks is essential, and a crucial function of INTELPOL is, precisely, on determining the levels of risks associated with threats that may compromise police missions and activities.

3.1.2.3 Planning

Public Safety and Order connected with mass gatherings are essential areas of INTELPOL, oriented to the identification and timely determination of the levels of risks that affect society, high entities, infrastructures and major events in order to prevent their materialization, being an essential element in the support to the planning and the adequate affectation of police resources, in particular, with respect to Public Order.

In Public Order, the determination of the level of risk is fundamental at the planning stage, allowing the decision-maker to anticipate the context in which it will act, to know the vulnerabilities and the potential consequences of the unfolding of the event. INTELPOL is therefore a crucial component of this type of operation, especially because it is capable of adopting a proactive approach in the investigation of information, before the mass gathering event, with the aim of analysing the risks of illegal actions and thus avoiding that the mass gathering deviates from its initial assumptions and becomes violent.

In fact, the international doctrine, both regarding security management of major events and the specific one on demonstration policing, is consensual in the extreme relevance that the role of INTELPOL has in its planning and execution, being essential to identify and manage the associated risks, especially those that are particularly complex.

4 Guidelines for Security Policy Specification

There are 12 main elements3 presented to policy makers and security planners essentials for develop an effective strategy when planning major event security.

4.1 LEADERSHIP/GOVERNANCE

It's indispensable the appointment of the one that will have the effective responsibility for the event security. That one should also have the power to decide and establish the command protocols or contracts that will enunciate exactly who has responsibility for planning and delivering what, where and when. The way in which responsibilities for the security are divided up should be formalized in detail and agreed upon by the authority in charge of the security. It is extremely useful that all security agencies involved properly understand the chain of command and their specific responsibilities.

Major events need both leadership and management. Leadership is about establishing direction and developing a vision that aligns and inspires a group of people. Management is about realizing the vision and strategy delivered by leaders, directing and staffing the tasks, handling day-to-day problems and monitoring outcomes.

It is therefore significant that authority carries together strategic, tactical and operational level commanders.

- **Strategic commanders** have responsibility and accountability for the operation and should maintain a strategic overview and not become overly involved in tactical level decision making. They should also ensure that the strategy is documented in order to provide clear audit trials.
- **Tactical commanders** are responsible for evaluating all available information and intelligence, applying professional judgement, coordinating and briefing allocated resources, developing plans and reviewing and refining progress to achieve the strategic objectives within the range of approved tactical options.
- **Operational commanders** are lastly responsible for managing the implementation of tasks identified at tactical level within their specialist and/or geographical area of responsibility. They should be knowledgeable of the tactical plans and their role within them and keep tactical commanders updated on any developments. Commanders at all levels should be properly located to maintain effective command within their area of responsibility.[4]

4.2 PLANNING STRUCTURE AND MANAGEMENT

This workout normally starts with the research on the policing of previous major events using a critical assessment. This research include, as an example, the identification of best practice for policing major events and an analysis of tactics used by demonstrators. After that, we need to appoint senior planning staff members dedicated to the operation. This team will seek to identify the main branches such as

- Intelligence
- venue security
- traffic management
- public order

[3] IPO Security Planning Model it's used in Portugal when PSP have security responsibilities during the development of a major event.

[4] IPO Security Planning Model

- logistics
- human resources
- command and control
- etc.

All the identified branches will conduct to the Master Plan.[5]

Strategic, tactical and operational commanders need a suitable structure to support their activities. It is unlikely that major events can be secured within an existing organizational structure. The scale and complexity of the event requires the involvement and integration of different agencies at local and national levels to form a unified entity.

Effective management and coordination of resources depend on the connection of more than just one LEA and might, for example, include diverse ones:

- Public security police
- Judicial police
- Criminal police
- Intelligence services
- Border control officials
- Fire and civil protection services
- Civil aviation authorities
- Maritime authorities
- Medical emergency institutes
- Public health officials
- Others.

4.3 INTELLIGENCE

- The intelligence structure will include representations of a wide range of relevant agencies on local, national and international levels to develop a comprehensive intelligence system for gathering, analysing and disseminating intelligence and information to help policy makers, security planners and others (e.g. border control officials) to identify threats, vulnerabilities and risks. The system includes:
- **Threat assessment**: The likelihood or probability that potential threats such as terrorist groups, criminals or mentally disturbed individuals will attempt to attack a particular target such as a person or a building within a specific timeframe.
- **Vulnerability assessment**: The possible vulnerabilities of a target which could be exploited in an attack.
- **Risk assessment**: The likelihood or probability that potential threats will attempt an attack by exploiting the target's vulnerabilities.

[5] IPO Security Planning Model

Risks can't be totally eliminated but they can be significantly minimized and contained. It is therefore important to develop a risk assessment approach to identify the most significant risks and determine suitable measures to manage them.

4.4 MEDIA & PR STRATEGY

Provide a coordinated, accurate and timely information is a very important component. It is crucial to deliver security related information and public support, as well as to have the media up-to-date. Media monitoring it's also a key element as is the contingency planning of media replies in the event of a crisis. With this purpose, it is imperative to:

- Assign a public information strategy that provides the community, participants and spectators with a range of security related advice and information about items such as recommended routes, road closures and access restrictions.
- Offer public reassurance to clarify in simple terms why certain short-term limitations may be indispensable.

4.5 VENUE SECURITY

Project the security plan for the controlled venue area. The main goals associated with this step are:

- **Hardening the designated secure area:** Identifying the designated secure area around the venue(s) and strengthening that area with human, physical and technical reply options. When appropriate, the security areas can be protected by physical and technical means, i.e. fences, anti-vehicle barricades, anti-terrorist barriers and gates, etc. There are also other measures that can help harden secure areas, such as movement sensors, extra blockages, setting light angles and sources to illuminate the designated area, watch towers, stationery guard points, foot and mounted patrols, plain-clothes officers, alarm systems, CCTV with infra-red capability, wireless communications sets, etc.[6]

[6] IPO Security Planning Model

Examples of checklist questions

- Are there enough security layers, rings and zones to protect the venue?
- Would the physical and non-physical barriers stop attacks by identifying threats?
- Is the buffer zone area sufficient to protect the inner area from the effects of a bomb attacks etc. on the outer cordon?
- Are personnel on Vehicle Screening Area (VSA) properly qualified?
- Are CCTV cameras properly located?
- Are anti-intrusion systems likely to withstand environmental factors?
- Are there any constraints around the building cordons, such as permission from landowners to build, aesthetics, environmental impact, etc?

Checklist 1 Hardening the designated area

- **Search, seal, secure and keep secure:** Carrying out a systematic search to negate risks from items such as improvised explosive devices, firearms, CBRN materials or other weapons of attack, possibly secreted on, above or below the event site(s). The aim is to search, seal, secure and keep secure the designated area by carrying out a systematic search for improvised explosive devices, firearms or other attack agents, possibly secreted on, above or below the event site.[7]

Examples of checklist questions

- Are there sufficient personnel trained to search all event sites?
- Are personnel properly qualified and experienced?
- Has enough time been allocated for the site to be thoroughly searched?
- What is the process in the event of a "find"?
- Has an air exclusion order been applied for?
- Are plans to neutralise challenges to security at cordons and access points comprehensive?
- Are there measures to block snipers' "lines of sight"?

Checklist 2 Search, seal, secure and keep secure

[7] IPO Security Planning Model

- **Public safety maintenance:** Identifying a range of complementary operational policing strategies, tactics and plans to protect life and property, deliver a safe, secure and uninterrupted event, if necessary, facilitate lawful protest. The aim is to apply adequate policing strategies to ensure a secure and uninterrupted major event, facilitate lawful protest and, when necessary, organize proactive engagement with individuals or groups challenging the security measures. LEA's should be prepared to consider a wide range of tactical options such as having designated areas for dispersal, the use of barriers for isolation and containment, arrest and control, arrest and processing procedures for compliant, non-compliant and disabled subjects, the use of dogs, and the use of less lethal options such as chemical agents, water cannons, Taser and baton rounds.[8]

Examples of checklist questions

- Are there police tactical options to deal with protester tactics such as the use of balloons to fly over areas with a message, the use of banners to make statement, the use of para gliders to attract publicity, barricades, dumping sand, obstructing access, the use of vehicles as a "go slow", disinformation, the use of e-mail or fax to blockade a target by overwhelming their IT system, damage to property, guerrilla gardening, the use of explosive as incendiary devices or smoke bombs, harassment, incursions, infiltration, lock ons and marches?
- Are each of the police tactical option legal?
- Are there strategies for early intervention to prevent disorder?
- Are contingency plan in place to deal with routine crime matters?

Checklist 3 Public safety maintenance

- **Vetting/Ticketing:** Designing systems to prevent infiltration of the venue event by persons who are not authorized through a process of vetting, validation and accreditation. Staff, athletes, delegates and other non-ticketed people should be properly identified and appropriately accredited for the location in which they are permitted access. The extent of the vetting validation and accreditation process and who carries out the process or parts of the process varies significantly from the event to event. Ticketing is the setting of policy for ticketing sales, collecting tickets, recognizing the identity of ticket holders and preventing potential perpetrators from buying tickets.[9]

[8] IPO Security Planning Model

[9] IPO Security Planning Model

Examples of checklist questions

- What are the procedures when fraudulent accreditation is discovered?
- Will accreditation databases manage the volume of work?
- Are personnel trained to work with the database?
- Was the technology effective when used at prior events?
- What is the process for lost or stolen accreditation?
- Are late accreditation procedures effective?
- Are systems in place to detect forgeries?

Checklist 4 Vetting/Ticketing

- **Access Control:** Identifying venue access and egress points for different categories of persons, including principles delegates, media, participants, spectators, etc., to control entry and deny access to unauthorized people, those with prohibited items, and anyone else prohibited from entering for any other reasons. In some types of event, a separation of access and egress points can be a useful means to manage the flow of people.

Examples of checklist questions

- Are there tactical operations to conduct inspection of vehicle, luggage, bags, equipment and material likely to be effective?
- Would the measures discover and deny access to individuals using false accreditation?
- Are the personnel doing body searching and frisking at access points experienced?
- Are there contingencies to deal with finds of explosives and other threats?
- Are there contingencies to deal with suicide bombers?

Checklist 5 Access Control

- **Dignitary/personal protection:** Designing additional security arrangements for designated categories of participants such as dignitaries and VIPs etc. These are precautionary, preparatory and proactive measures that ensure the security of individuals deemed to be at risk.[10]

[10] IPO Security Planning Model

Examples of checklist questions

- What are the specific threats related to those requiring protection?
- What are the procedures for the evacuation of principals?
- Are there contingency itineraries, routes and travel schedules?
- Is the composition of motorcades appropriate?
- Will foreign protection officers be entitled to carry firearms?

Checklist 6 Dignitary/personal protection

In conclusion, a set of security plans must be considered that ensure:

- Save life, protect property and prevent crime inside the designated secure area (inside),
- Save life, protect property and prevent crime outside the designated secure area (outside),
- To be prepared in security related contingency planning terms (if).

Figure 1 illustrate how in each of the three main categories of complementary plans ('inside', 'outside' and 'if') - which people need to be protected, where they have to be protected and how they can be protected.[11]

[11] IPO Security Planning Model

	Who to protect	What to protect	How to protect
Inside	• Participants • Spectators • Security and non-security staff	• Event venues	• Securing and hardening the secure area • Search and surveillance • Cordon control • Vetting • Access control • Dignitary protection
Outside	• Community • Participants • Spectators • Security and non-security staff	• Country access points (land, sea and air) • Access routes to and from the event venues • Event related sites • Critical Infrastructures • Other vulnerable and soft targets	• Traffic management • Border control • Intelligence-led policing • Protection of non-event and event-related sites
If	• Community • Participants • Spectators • Security and non-security staff	• Inside and outside the event venues	Have plans and responses for: • Major Incident Contingencies • Public Safety Contingencies • Arrest & Court Arrangements • Airport Contingencies • Crime Contingencies • Transport Contingencies • Communication Contingencies

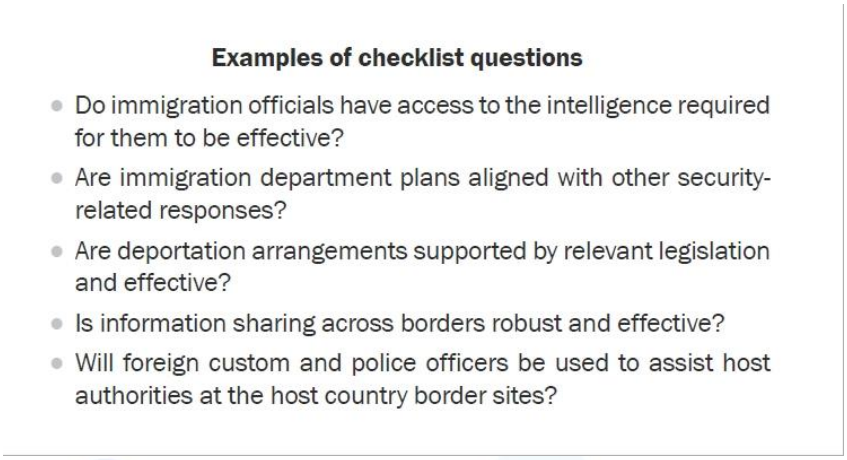
Figure 1 Security plans for venues (Who, what and how; inside, outside, if)

4.6 BORDER CONTROL

During the designated period of a major event, consideration could be given to strengthening routine border control activities to:

- Provide at the earliest possible opportunity an effective intelligence-led response.
- Detect and possibly prevent the entry of individuals seeking to disrupt the event in any way.
- Detect and possibly prevent a range of event related illegal activities.
- Provide opportunities to enhance information sharing and the collection of event related information and intelligence.[12]

[12] IPO Security Planning Model



Checklist 7 Border Control

4.7 TRAFFIC MANAGEMENT

The aspect of traffic management must consider the following key points:

- Sustain and protect access routes to and from venues and other designated places for stakeholders in general, which includes the management of road closures and other tactics involving for instance, the saturation and securing of critical and alternative routes.
- Conserve and secure a viable road network throughout the security areas and beyond. This may involve the suspension of roadworks, securing bridges and tunnels, reviewing the speed limits and other forms of traffic control.
- Project a public transportation system that is capable of handling expected volumes of people at given times and places in a safe and secure way.
- Develop contingency plans to deal with incidents that may occur on the national and local road network such as the disruption or the blockage of routes by accidents, protesters or any other incident.[13]

[13] IPO Security Planning Model

Examples of checklist questions

- Are the plans developed for hazard events related to transport such as congestion, accidents and terrorist attacks likely to be effective?
- Has consideration been given to signposting, timing, traffic-flow, traffic restriction orders, speed limits etc.?
- Are the transportation plans sufficiently flexible to allow for changes and emergencies?
- Has the transportation plan been adequately tested before the major event and did it work?

Checklist 8 Traffic Management

4.8 NON-EVENT AND EVENT RELATED SECURITY

Extend the security blanket outwards from the designated secure venue site(s) and design a range of strategic and tactical options to further enhance the likelihood of meeting the key objectives for the security operation. In particular, such plans should include appropriate measures to prevent crime and protect people and property. Possible targets include event-related sites such and critical infrastructures. The protection of soft targets[14] should also be considered[15].

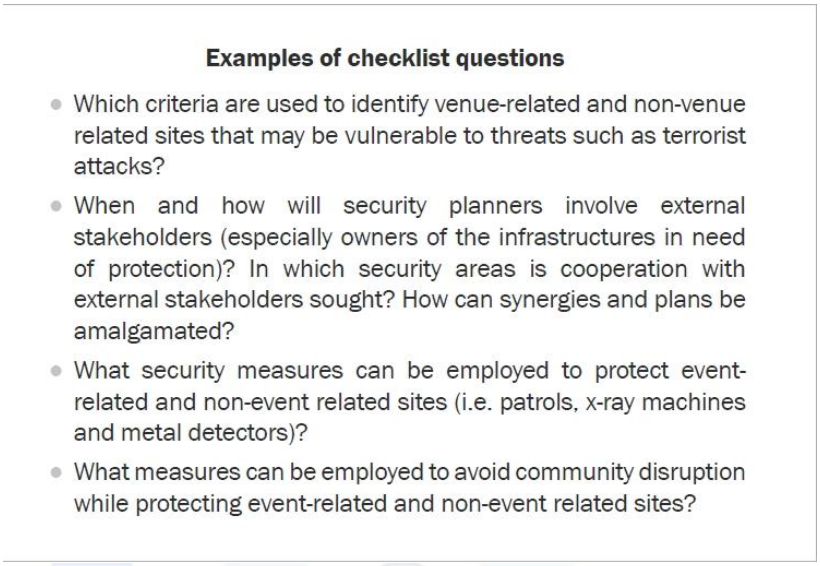
There are some main basic steps that should be considered by security planners:

- **Assessment:** Identification of those event-related and non-event related infrastructures and assets that could become vulnerable during the major event in terms of national-level public safety and security.
- **Awareness:** Promotion of awareness amongst all stakeholders of the potential for and impact of an attack against the critical infrastructures. It is important to establish a proactive environment where public authorities, private sectors and private citizens can cooperate through a multi-agency approach.
- **Protection:** Deployment of an early warning mechanism for attacks against event-related and non-event related sites and enhancement of law enforcement counter-attack capabilities.[16]

[14] Such as shopping centers, tourist sites and historical monuments.

[15] Making a retrospective, nowadays soft targets are considered the preferred aims of terrorist activities taking into account the high concentration of people and the lightness of existing security measures when compared to critical infrastructures.

[16] IPO Security Planning Model



Checklist 9 Non Event and Event Related Security

4.9 HUMAN RESOURCES AND LOGISTICAL SUPPORT

Identified operational requirements, contemplate populating security plans with human, physical and technological resources, ensuring:

- Backup the strategic objectives of the plan with adequate personnel who are properly trained, equipped and experienced in terms of the role they are expected to fulfil and comprehensively briefed in this regard prior to the deployment.
- Giving adequate logistical support in terms of matters such as catering, accommodation and transport.
- Improving the human aspects of the response with reliable equipment and technological solutions such as CCTV, sensors, detectors and means of communications.
- Planned withdrawal of personnel, equipment and security measures after the event.
- Return to normality.[17]

4.10 INFORMATION TECHNOLOGY (IT) AND COMMUNICATION

Establish communication schemes proficient enough to satisfy the needs of the operation, including:

- Communication and IT design: instituting real and positively secure radio, telephone and other means of communications to all organizations and agencies involved in the security of the major event.
- Communication and IT controls: guaranteeing that power supplies can be preserved, command centres and crisis rooms are suitably sited, and that systems and IT security solutions are tested before the event.

[17] IPO Security Planning Model

- Communication and IT procedures: instituting a clear framework of information flow procedures so that everybody involved will know who should inform whom of what and when.
- Communication and IT protection: designing and implementing plans to protect core communication infrastructures and have prepared plans to maintain communications in case of crisis conditions.

4.11 INTEGRATION AND COORDINATION

Constant course to certify that all the partitions of planning are combined, balancing and synchronized:

- Check the integration, complementarity and flexibility of plans and their efficiency.
- Check the capability of the individuals and teams.
- Check safety and security procedures to guarantee they are ranged with ordinary operation processes.
- Check equipment is appropriate.[18]

4.12 CONTINGENCY PLANNING AND CRISIS

It's mandatory to develop contingency plan for crisis. Those contingency plans should consider some basic principles such as:

- Combined and coordinated management: contingency plans should be based on a multi-agency approach that includes event organizers, police, health authorities, fire authorities, local authorities, private sector organizations (transport, utilities, etc.), stewards and first aiders. It is important to allocate specific duties and responsibilities during the planning phase. Crisis management structures must clearly define roles and responsibilities at all levels. The procedures should be written and available for all participating agencies. Instructions should be specific and easily understood.
- Assessment: Factors that need to be considered while designing contingency plans include characteristics of the event (type of event, audience profile, location of the venue), identification of emergency routes, identification of ambulance loading points, location of hospitals, emergency equipment availability and location, consequences of a given attack, etc.
- Response: Contingency plans should prepare a range of options and scenarios to deal with specific issues. It's impossible to generate a single model to respond to every emergency, therefore responses must be flexible and vary rendering to the nature and effects of the crisis. Common objectives:
    - Saving and protecting life and property.
    - Treating, rescuing, and transporting casualties.
    - Containing the emergency and the casualties.
    - Managing evacuation.
    - Cancelling or stopping the event.
    - Safeguarding the environment.
    - Maintaining critical services.
    - Providing the media with information.

[18] IPO Security Planning Model

- Restoring normality as soon as possible.
- Ensuring scenes and evidence are preserved.
- Facilitating investigations and inquiries.[19]
- Training and exercising it's quite relevant to test the efficiency of plans and the competence of all people involved. It is also important to schedule training exercises and use progressive training.[20]

Examples of checklist questions

- Have all types of accidents have been planned (fires, natural disasters, collapse of constructions, power outage, etc)? Are there specific event-related emergency plans? Are all staff trained for the procedures in case of an emergency?
- Are evacuation plans and procedures up-dated, tested and trained to control crowds after incidents occur? Is there a designated emergency evacuation route?
- Have emergency services such as fire departments practiced with the venue organization team in case of an emergency?
- What security incidents are planned for on the site-level? Is the site a potential terrorist target (e.g. because of its location, history, symbolic significance etc.)?
- Does the venue have its own resources to respond to emergencies?
- Are there resources to deal with extraordinary threats such as CBRN (stockpile of drugs to counter chemical and biological agents in small quantities for first responders on site; new technologies and new equipment used to detect possible attacks with chemical, radiological or biological weapons, etc)?

Checklist 10 Contingency planning and crisis

[19] IPO Security Planning Model

[20] IPO Security Planning Model

5 Conclusions

This deliverable has set guidelines for security policy specification, after defining key aspects of decision making, planning and risk calculation for mass gatherings.

This is the first version of a total of 2 deliverables that address security policy specification.

This version is focused on PSP methodologies:

- How they make decisions
- How they plan the covering of a mass gathered event
- Which are they key aspects for planning pre-event and event execution phases
- How they calculate risks
- Which are their guidelines for security policy specification

This first version helps knowing better what some guidelines are for LEA's when they have to cover an event. Nevertheless, it may not represent the entire EU for this context. This is known to be this way in the first version of Security Policy Specification.

Version 2 will address the same topic from different perspectives and with the vision of other LEA's around EU.

After carefully reading the Guidelines and together with D4.2, a set of fields and key taxonomies can be extracted to properly build the model for PMT tool. Also, the entire document is helpful as a guideline to implement the PMT tool.

6 Acronyms

Acronyms List	
LEA	Law enforcement agent
INTELPOL	Police Intelligence (Tool)
EU-SEC	European Security Certification Framework
EUROPOL	European Union Law Enforcement Agency (European Police)
PSP	Polícia de Segurança Pública (Portugal Public Security Police)
EU	European Union
PMT	Policy Making Toolkit (LETSCROWD Tool)
IPO	International Permanent Observatory

Table 1 Acronyms