| Title: | Document Version: |
|---|---|
| D4.7 Security policy specification | 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*: |
|---|---|---|
| M | M | RE |

*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)
Jordi Arias (ETRA)
Gorka Sanz (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 | 31.01.2019 | First version | Pedro De Brito (PSP) |
| V0.2 | 07.02.2019 | Review | Alexis Gizikis (EENA) |
| V0.3 | 11.02.2019 | Review | Jordi Arias (ETRA) |
| V0.4 | 13.02.2019 | Second version | Pedro De Brito (PSP) |
| V1.0 | 15.02.2019 | Final version after peer review process. | Jordi Arias (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 (LetsCrowdServer).

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

When security planners first try to list everything that an authority needs to do to prepare for a secure event, they soon realise that the list of issues to be addressed is long and heterogeneous. For example, it is important to understand who will be responsible for which aspects of security at different locations, how the planning effort will be structured, how interagency cooperation amongst public safety agencies at different levels of government will be managed, the role of private security companies, and how the media will be managed. The list goes on, but in short, planning the security of a major event is largely about coping with complexity.

In this sense, the present deliverable tries mostly to point out and highlight the main components of the planning process and the guiding principles that underpin the provision of security at major events.

## 1.2 SCOPE OF THE DOCUMENT

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

The Deliverable 4.3 was related to the methodologies used by the PSP, specifically regarding the decision-making process, planning and risk analysis in the management of major events, presenting the main lines used.

At the time of production of the first version, we proposed to carry out a subsequent analysis of the guidelines used by the remaining LEAS partners of the project. Subsequently, it was concluded that only PSP has national responsibilities in this area, and the other partners have a municipal or regional character, and some of them have no public order competences.

In this perspective we have pointed out our efforts for the Europe, and it was possible to conclude that, like Portugal, a substantial part of the European countries also assumed the premises of the IPO Security Planning Model and later in the EU-SEC, considering that they participated in its elaboration.

For those reasons we have decided to complement the work presented in the first version, using the same structure and points carried out, special the ones that we have considered to be 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 LEAs build a decision, plan the pre-event and execution phases of the event and calculate risks to prevent and mitigate incidents.

Once definitions are clear, a section with current tools describes how LEAs should address the complex problem of deciding and planning an event using INTELPOL, at national and international level.

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 making.

The conclusions describe 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.

Nevertheless, even taking into account other factors, namely the cost and the economic impact, what emerges from the study developed in this field is that planning the security for a major event is a very intricate exercise that involves a variety of processes and accomplishments.

## 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. In major events, the decision maker has to do anticipation of scenarios in order to find alternative solutions with regard to the changing of events on the field. So, any plan benefits from knowledge coming from available intelligence and from the decision makers’ experience.[2]

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.

In this sense, it’s normally considered that the intelligence gathered before and during the event (because the risk assessment has to be made constantly through the intelligence structure) will empower the decision maker to achieve a higher operational result and, in consequence, ensure a superior level of

[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.

[2] SCHWENKER, B. e WULF, T. (Eds) (2013). Scenario-based Strategic Planning: Developing Strategies in an Uncertain World. Munique: Springer Gabler.

security for the masses during the major event. The intelligence structure of PSP has the responsibility to inform the decision maker with all types of relevant data needed to pursuit a high level of operational and tactical outcome.[3]

The intelligence structure has the main objective to control the information released to the decision maker, for instance, the confirmation of the source and the liability of the information are necessary, before creating a product to be released for the Police commander (decision maker). The Police commander has the need of relevant information that allows to prepare a major event, flawless and accurate.

It is important, nowadays, to maximize the information exchange between the different countries due to, as known, the international threats can be materialized in every single part of the globe.

### 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 decision maker, namely: guarantee the exercise of fundamental rights; manage proportionality and adequacy of police intervention; assess risks; decide on preventive interventions.[4]

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.[5]

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[6]. The evaluation of the information of the event within this project will be made in a module

[3] FERNANDES, L. (2014). Intelligence e Segurança Interna. Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna.

[4] FERNANDES, L. (2014). Intelligence e Segurança Interna. Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna

[5] WATSON, R. e FREEMAN, O. (2012). Futurevision: scenarios for the world in 2040. Melbourne/Londres: Scribe Publications.

[6] SCHWENKER, B. e WULF, T. (Eds) (2013). Scenario-based Strategic Planning: Developing Strategies in an Uncertain World. Munique: Springer Gabler.

called Policy Making Toolkit and it is based in the comparison between the registered policy laws and the information of the event, this tool will be explained in deep in the D4.8.

In order to improve the success of each operation regarding Major Events it is important to consider the possibility to make, in all major events, a summary of past procedures regarding problematic and challenging circumstances that occur during the event to improve the upcoming ones, to be able to learn with the mistakes or successes from the past.

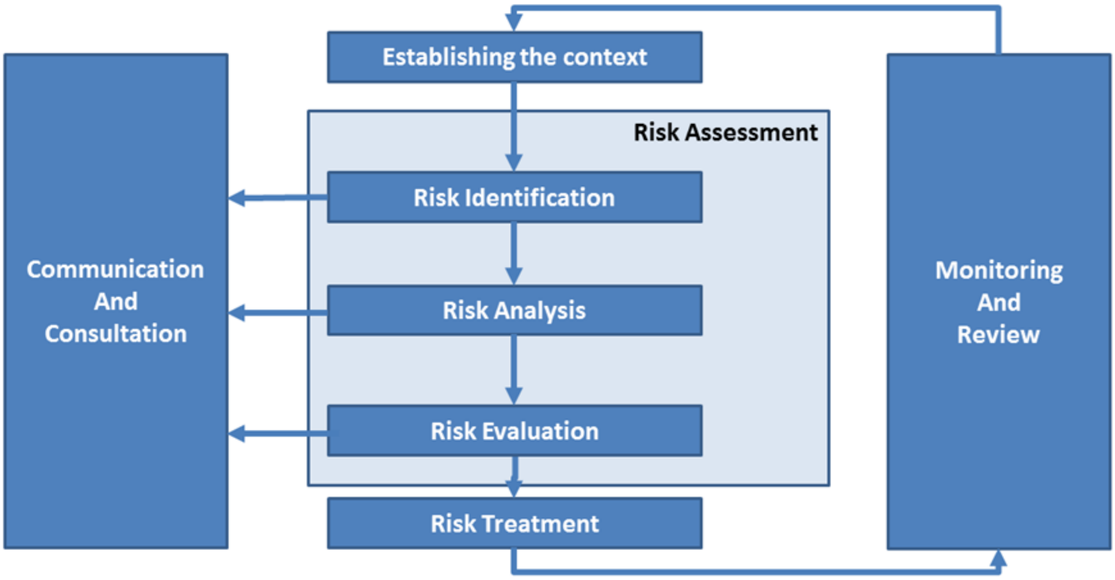
This kind of “brain storming” exercise regarding all the operation for a major event since the gathering of intelligence to the execution of the operation towards a successful result has showed to be important in some structure in order to achieve even better results in the next major event, increasing the success rates regarding the preparation and execution of such events.[7]

### 2.2.2 Risk Management

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.

Risk management is an important tool for decision makers support their choices and allow them to prioritize actions and distinguish between different options. According to ISO 31000:2009[8] risk management process is constituted by three parts, which are “Establishing the context”, “Risk assessment” and “Risk treatment” (Figure 1).



[7] CLARK, R. (2010). Intelligence Analysis: A Target-Centric Approach (3ª Edição). Washington: CQ Press.

[8] ISO 31000 – Risk management – Principles and guidelines.

Figure 1 – Risk management Process (Adapted from ISO 31000)

In the first step, which is "Establishing the Context", we define the external context, like social, cultural and political situation. This dimension should be analysed at an international, national, regional or local level. On the other hand, when we talk about internal context, we are looking at the organization's culture, processes, structure, and strategy. When we are establishing the Context, it is important to define a risk criterion, according to the organization's values, objectives, and resources.

The risk management process second step is a Risk assessment. This process stadium is another sub process that includes three phases: (a) Risk identification; (b) Risk analysis; (c) Risk evaluation.

(a) Risk identification: analysts should identify "sources of risk, areas of impacts, events and their causes and their potential consequences"

(b) Risk analysis: analysts should consider the causes and sources of risk, their positive and negative consequences. At the same time, analysts should measure the likelihood of those consequences. The combination of consequences and likelihood determinate the risk level. The analyses could be qualitative, semi-quantitative or just quantitative.

(c) Risk evaluation: analysts should assist decision makers, based on the outcomes of risk analysis, about which risks need treatment and the priority for treatment implementation. According to the ISO 31000:2009 "the risk evaluation can lead to a decision to undertake further analysis"[9]

For last, the third step about Risk management process is Risk treatment, which involves another process, where it is assessed a risk treatment solution and it is decided if the residual risk level is tolerable. The outcome of this process can be: 1) avoiding the risk; 2) taking or increasing the risk in order to transform it into an opportunity; 3) removing the risk source; 4) changing the likelihood; 5) changing the consequences; 6) sharing the risk; 7) and retain the risk by informed decision. There has been developed a complex algorithm for evaluating all the possible input risks and evaluate an event based on it, this algorithm will be explained in deep in the D4.8.

### 2.2.3 Planning

Planning embodies and reflects a given decision-making process and materializes in the elaboration of a plan. Planning is focused on decisions and activities that assess threats, identify preventive measures, develop response and recovery actions and coordinate resources and the command control, as well as communications elements required to solve an incident if it is necessary[10].

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 plans produced can be categorized into several broad categories like transportations plan, crowd movement plan, event operations plan, safety and security plan and media/information plan[11].

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.

[9] ISO 31000 – Risk management – Principles and guidelines.

[10] NCS, (2017). Project STADIA. Sports security Senior Management Training Course

[11] NCS, (2017). Project STADIA. Sports security Senior Management Training Course

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.[12]

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.[13]

An effective intelligence and information sharing strategy is a fundamental component of a proper security plan.[14]

The failure to carefully consider each course of action and how it will impact the desired outcome and can result in an increase the confusion, waste of time and resources, increase risks to life and property, and slow resolution of the incident. After considering the most probable scenarios the Police Commander, assisted by his subordinates, will deploy the human and material resources in order to be able to prevent, or if not possible, to respond effectively to a public order altercation.

The planning of a mass gathering event is always to prevent all kind of incidents or, if incident occurs, it is expected that authorities are able to restore the public order and the people safety and security in a smaller window time with the smallest problem for the ones gathered in the event. So, regarding this subject it is possible to understand the importance of intelligence data and the production of different and probable scenarios in order to be able to prevent of respond any kind of threat or public order altercation.[15]

[12] BAS, E. (2010). Prospectiva – Cómo usar el pensamento sobre el futuro. Barcelona: Editorial Ariel, S.A.

[13] WEICK, K. e SUTCLIFFE, K. (2007). Managing the Unexpected: Resilient Performance in an Age of Uncertainty (2ª Edição). São Francisco: John Wiley & Sons, Inc.

[14] GRABO, C. (2010). Handbook of Warning Intelligence – Assessing the Threat to National Security. Plymouth: Scarecrow Press, Inc.

[15] LINDGREN, M. e BANDHOLD, H. (2003). Scenario Planning: The link between future and strategy. Nova Iorque: Palgrave Macmillan.

# 3 State of the art: Existing tools and methodologies

## 3.1 POLICE INTELLIGENCE TOOL (INTELPOL)

Grounded on the experience of many years dealing with mass gatherings, a great part of an LEA with public order competences apply to the police intelligence (INTELPOL) as one of the most relevant instruments used to spot evidence-based indicators that would help decision-makers.

### 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.[16]

The INTELPOL should provide:

(a) 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.

(b) 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.

(c) 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.[17]

### 3.1.2 Functions for decision making and intelligence

As it turns out, one of the primary functions of INTELPOL[18] 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.

To achieve this goal, it is important to consider the intelligence cycle to understand all the process of intelligence that is made before an outcome is presented to the decision maker. So, the intelligence cycle is made up of five interdependent functions: (a) Planning and Direction; (b) Collection; (c) Processing; (d) Analysis and Production; (e) Dissemination.

(a) The first step is planning and point the direction of the task to be done, this is the most important of all, because of influences all the rest. It is needed to define and begin planning what we'll do and how. At this stadium, the decision makers point to a specific direction and the analysts list what they know about the issue and what they need to find out.

(b) The second step is to collect information overtly (openly) and covertly (secretly). Reading foreign newspapers and magazine articles, listening to foreign radio, and watching overseas television broadcasts are examples of "overt" (or open) sources for us. Other information sources can be "covert" (or secret).

[16] FERNANDES, L. (2014). Intelligence e Segurança Interna. Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna

[17] UNICRI, IPO Security Planning Model, 2007

[18] FERNANDES, L. (2014). Intelligence e Segurança Interna. Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna.

(c) After analysts collect all the information, they will process it by putting it into an intelligence report.

(d) The fourth step is analysis and production, where we assess what is happening, why it is happening, what might occur next, and how it affects organization interests.

(e) The fifth step is dissemination, where we give our final written analysis to the decision maker, the same who started the cycle. After reading the final analysis and learning the answer to the original question, the decision maker may come back with more questions.[19]

#### 3.1.2.1 Police Decision Process[20]

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 important information to the decision makers.

#### 3.1.2.2 Risk Management[21]

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.

As said before, the Police resources are limited so the risk management is essential to maximize the police actives distribution on the field during the operation, allowing the decision maker to mitigate the risks.

#### 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.[22]

In the pre-event planning, intelligence and information-sharing constitute the basis for risk assessment. The decision maker should decide in advance if intelligence and counter-intelligence operators are needed in the field during an event. Information from field-level should flow from intelligence operators to the decision maker.

[19] FERNANDES, L. (2014). Intelligence e Segurança Interna. Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna.

[20] GRABO, C. (2010). Handbook of Warning Intelligence – Assessing the Threat to National Security. Plymouth: Scarecrow Press, Inc.

[21] ISO 31000 – Risk management – Principles and guidelines.

[22] HEUER, R. e PHERSON, R. (2011): Structured Analytic Techniques for Intelligence Analysis. Washington: CQ Press,

Having the technology and staff on duty for data mining social media sources prior to and during an event has become a recognized best practice.

The planning is defined in six steps: 1) Evaluate the situation; 2) Establish goals and objectives; 3) Determine potential courses of action; 4) Complete, review and approve the plan; 5) Issue orders and execute the plan; 6) Monitor progress and make refinements.[23]

[23] NCS, (2017). Project STADIA. Sports security Senior Management Training Course

# 4 Security Guidelines for Security Policy Specification

There are some guiding principles for law enforcement for planning and managing security for major special events that must be, at this point, highlighted.

Of course those guidelines aren't all-inclusive; it presents, in general terms, the highpoints of special event security planning and management, but there are obviously many more procedural and technical details involved in each area that will be appointed in specific terms.

- Ensure that timely and effective planning, communication, and training are prioritized. Jurisdictions handling special events on a routine basis should consider building events security training into basic and in-service training;
- Understand that overall management of special events is temporary—it involves developing new organizational arrangements, new relationships, and new structures. The key challenge in this context is to forge new relationships in a time-limited way that can bridge difficult challenges. This may be the key challenge in the entire safety and security operation.[24]
- Plan for and manage for the worst-case scenarios—extraordinary crime (and depending on the event, extreme protestors activities) and possible terrorist attack—but really be prepared to deal with the most ordinary and mundane crimes (pickpockets, thefts from autos, and vandalism) and common civil disruptions (fighting, drunkenness, and disorderly conduct).
- Anticipate unplanned activities and spur of the moment gatherings, for example, on the eve of a major event.
- Secure all perimeters including those in outer areas. In large special events, law enforcement must secure a series of perimeters (inner, middle, and outer). These often involve specific facilities and well-defined territorial venues. However, law enforcement must also be responsible for safety and security in the theatre—the broader "unbounded" areas of the city where other events may occur or VIPs stay in hotels.
- Realize that law enforcement needs to be concerned not only with the safety and security of participants and the event venue, but also the economics of the event. Many events involve commerce, have a budget, and provide income to the local economy.
- Recognize the need for and benefits of leveraging resources and collaborating with other law enforcement agencies; public safety (fire/EMS); other city and state agencies (health, building codes, transportation, parks & recreation); and private security.
- Develop an effective interoperable communications capability if multiple agencies are involved in the field.
- Involve citizens and the business community in planning efforts.
- Ensure that the event continues safely and at the same time respect Constitutional rights including freedom of speech and assembly.
- Ensure that the rest of the jurisdiction receives essential law enforcement services, regardless of the size or importance of the event.
- Evaluate continuously and review operations and practices to update and improve security.
- Prepare an after-action report after each event.

[24] GREENE, J. et al. (2002), Safety and security at the Olympic Games in Salt Lake City, Utah. Washington, D.C., Bureau of Justice Assistance, U.S. Department of Justice.

- Ensure that appropriate State officials are informed in advance about events with national or international significance to guarantee State awareness and possible support.

There are 12 main elements[25] presented to policy makers and security planners essential for developing an effective strategy when planning a major event security.

## 4.1 LEADERSHIP/GOVERNANCE

Definitely, planning and implementing security for major events entails strong leadership and governance. Governance is the act, manner and practice of managing, coordinating and selecting the best options available to produce deliverables in a timely and effective fashion. Governance is the core of the organisation that leads plans and implements effective, sensible and pragmatic security measures for major events. It includes leadership, structure, coordination, internal and external communication and legacy.

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.

Functioning in a harsh deadline, in a multi-agency and often politically sensitive situation, with unusual assets, recurrent intrusion, a restricted budget and powerful inquiry throughout it can be hard. Consequently, before any tangible planning work starts, it is advisable to negotiate, settle and enact the nomination of someone with the leadership potentials, skills and experience required for such an important responsibility. Leaders will have to ponder extensive, solid and accurately about each element and estimate respectively while taking into account the risks, threats and vulnerabilities of the event.

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.

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.[26]

## 4.2 PLANNING STRUCTURE AND MANAGEMENT

[25] UNICRI (2007), IPO Security Planning Model

[26] UNICRI (2007), IPO Security Planning Model

We can understand the planning phase in three parts: Pre-Planning Phase, Planning Phase and the operational phase and for last the recovery or review phase.

In the Pre-Planning phase, the workout normally starts with the research on the policing of previous major events using a critical assessment. This research includes, as an example, the identification of best practice for policing major events and an analysis of tactics used by demonstrators. But essentially this phase is dedicated to gathering information and intelligence about the event. During this phase, the Portuguese Police conduct a proper risk, vulnerability and threat analysis, take into account that each event is unique and requires its own assessment.[27]

Once the threats, vulnerabilities and risk level are defined, another phase starts, and it is planning how we are going to prevent or mitigate these threats. This phase includes thinking about technology that can be used to help mitigate risks as well as the training our staffs needs to ensure they are ready for the mission. Above all, the planning phase is about to think about a targeted plan. At this phase, 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
- logistics
- human resources
- command and control
- etc.

All the identified branches will conduct to the Master Plan.[28]

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

[27] TORRES, J. (2015a). A Gestão contingencial de cenários de risco para a segurança pública. In: Valente, M. (Coord.). Ciências Policiais e Política Criminal (pp.141-165). Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna.

[28] UNICRI (2007), IPO Security Planning Model

- Public health officials
- Others.

Finally, the third phase starts when the event's day arrives, and if we did a good planning, the scenarios have been considered and for sure we will be prepared for doing the necessary adaptation in resources allocation.

The last phase that is the recovery or review phase is a time to ask what to do in a different way next time. This part of the event management process is always about learning for improving in the future events. It is important to pull together the team and debriefing each aspect of the plan, assessing what was more or less effective for the event.[29]

## 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:

(a) **Threat assessment**: The likelihood or probability that potential threats such as terrorist groups, criminals, mentally disturbed individuals or others will attempt to attack a particular target such as a person or a building within a specific timeframe. In the case of groups of potential perpetrators, threat assessments involve examining "desire" and "expectation" to establish intent and "resources" and "knowledge" to establish capability. Assessing intent means acquiring intelligence on the plans and preparations of persons or groups of perpetrators. Assessing capability means acquiring intelligence on the resources that individuals or groups have at their disposal.

(b) **Vulnerability assessment**: The possible vulnerabilities of a target which could be exploited in an attack. The identification of vulnerabilities is made in terms of weaknesses in a defence system. Such assessments would include an evaluation of all protective and precautionary measures taken. Vulnerability assessments need to take into account the plans of all parties involved.

(c) **Risk assessment**: The likelihood or probability that potential threats will attempt an attack by exploiting the target's vulnerabilities. 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.[30] 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.

Early in the major special event planning process, law enforcement needs to conduct a comprehensive threat and risk assessment regarding the special event in order to plan for possible situations and for this purpose, they analyse the following factors[31]:

- Size of the event (and resources available in the field office).
- Threat—includes known threats to the event, current levels of domestic and global terrorist activities, and the realistic degree of danger that known terrorist groups may pose to the event.
- Significance—some events have historical, political, and/or symbolic significance that may heighten concerns about the event being a target.

[29] TORRES, J. (2015b). Gestão de Riscos no Planeamento, Execução e Auditoria de Segurança. Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna.

[30] Cuesta, J.H. & Jarvis, N., (2004). IPO Closed-Door Meeting, Madrid.

[31] Conners, E. (2007). Planning and Managing Security for Major Special Events: Guidelines for Law Enforcement. Institute for Law and Justice

- Duration—events lasting for extended periods of time require more resources.
- Location—certain locations may be more inviting for attacks; the geographic dispersion of an event is also a factor.
- Attendance—who is attending (cultural, political, and religious backgrounds).
- Media coverage—events with national or international media coverage may provide an inviting stage with a large audience for attackers to make a "statement."
- Dignitaries—high-level heads of state and VIPs require more protection and resources because they are targets for attacks.

General guidelines[32] for performing the information collection phase of a threat and risk assessment of a major special event include:

- Assign responsibility for the assessment to an experienced and qualified assessor. In smaller events, this may be a one-person assignment. For major events, the executive team may ask each subcommittee to conduct its own assessment in its area of responsibility. Provide timelines for assessment reports.
- Obtain and review available information. This includes facility plans floor plans, diagrams, utility layouts, electrical, etc.); photos of the geographic area (maps, aerial photos); reports from previous events; agreements or contracts signed by the governing body with event staff; certificates of insurance; inspection reports of the facilities (fire, health, safety); existing facility evacuation and emergency plans; facility or event policies, rules, and regulations; list of assets and value; and more.[33]
- Assess the security plans of key event hotels and interview hotel security staff for plans.
- Conduct extensive site observations and surveys. Identify all venues, traffic routes, facilities, grounds, parking areas, etc., that need to be secured and protected. Examine the layouts at different times of the day (light, dark) and days of the week to observe varying traffic and pedestrian patterns, identifying vulnerabilities.
- Examine all forms of transportation that participants will use to travel to the event—airports, trains, buses, subways, etc. Identify vulnerabilities.
- Conduct interviews with key event planners in the governing jurisdiction and the event promoters because all these people have ideas and plans for the event and it is important to obtain their plans early on.
- Obtain threat intelligence information from intelligence sources. This may include the lead agency's own intelligence resources.
- Develop detailed participant profiles. Identify the full range of participants planned for the event in terms of dignitaries, VIPs, event staff, government officials, performers, spectators, media, protestors, etc. Identify any cultural, religious, and political aspects of participants that may be relevant to security.

## 4.4 MEDIA & PR STRATEGY

Provide 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

[32] TORRES, J. (2015b). Gestão de Riscos no Planeamento, Execução e Auditoria de Segurança. Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna.

[33] Conners, E. (2007). Planning and Managing Security for Major Special Events: Guidelines for Law Enforcement. Institute for Law and Justice

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, allowed objects on the venue, road closures and access restrictions.
- Offer public reassurance to clarify in simple terms why certain short-term limitations may be indispensable.
- During the event it's also fundamental to nominate a responsible for the contact with *media*, specially update and provide information to the community.

In this guideline it's necessary taking into account the importance of giving an immediate and efficient response when a crisis came up. A crisis is an incident that happens unexpectedly and usually not within the organization's control. A crisis can create three related threats: (a) public safety; (b) financial loss; (c) reputation loss.

In 2011, the Justice and Home Affairs Council of the European Union recognized that integrated emergency and mass crisis communication was an effective tool to minimize harm and enable citizens to be better prepared in a disaster. During and following an emergency incident, individuals seek information that is specific to them: "How does the incident affect my safety, my friends/family, my job, my community?" These questions need to be answered when communicating with each audience.[34]

There is no one best way to communicate in an emergency, so redundancy with multiple methods to deliver information is primary. The use of audible messages via public address systems, visual means such as electronic sign-boards, scoreboard messaging and enhanced fire alarm/notification systems are starting points in a plan. This means that the crisis Communication plan should involve identifying likely incident scenarios in advance to construct messaging templates to work from when an incident occurs.

It is important to establish credibility and control the message surrounding an incident, by having a formal press conference in a timely manner following the incident. It is important to release as much factual information as soon as possible.[35]

## 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.[36]
- If needed, and depending on the type of event, it can be important the inclusion of several zones with different types of controls or safety rings (usually 3) were it can exist several check points controlled by police, helped by private security.

[34] COUNCIL OF THE EUROPEAN UNION, (2011), Press Release n.º 18498/11, 13 e 14 de dezembro, Brussels

[35] NCS, (2017). Project STADIA. Sports security Senior Management Training Course

[36] UNICRI (2007), IPO Security Planning Model

- Besides the security of the venue and the surrounding area the city or town where the mass gathering occurs has always to be another important part of the operation. The plan and execution have to fulfil the necessity of providing the appropriated means outside the venue preventing criminal situations and response capacity besides the venue area. This important measure can also be vital to inform the decision makers about some situations that are happening outside the venue but that can but directly influence the event.

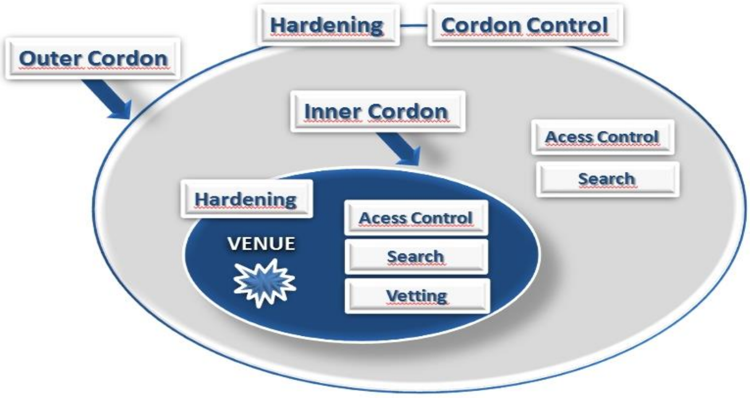
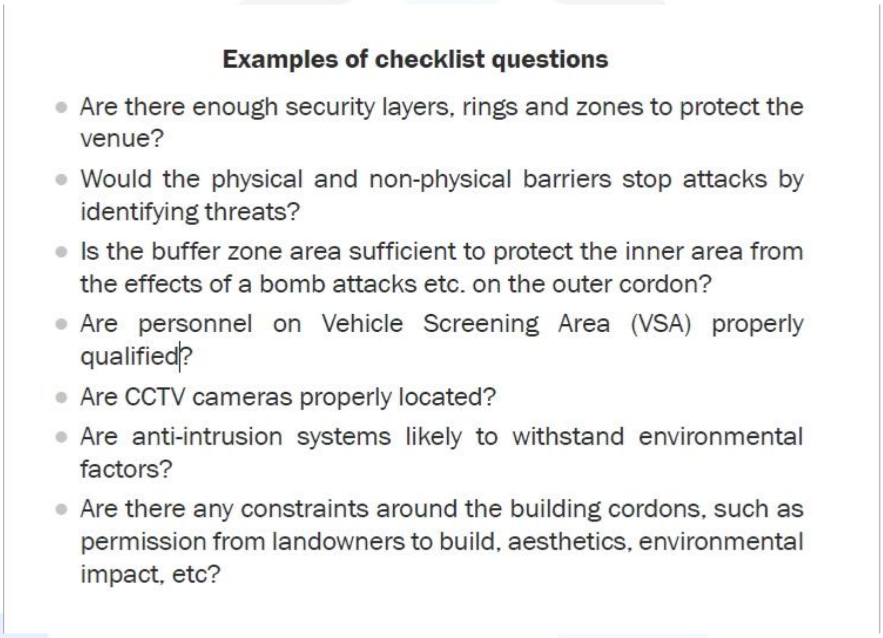


Figure 2 - Hardening the designated area (adapted for IPO Security Planning Model)



**Examples of checklist questions**

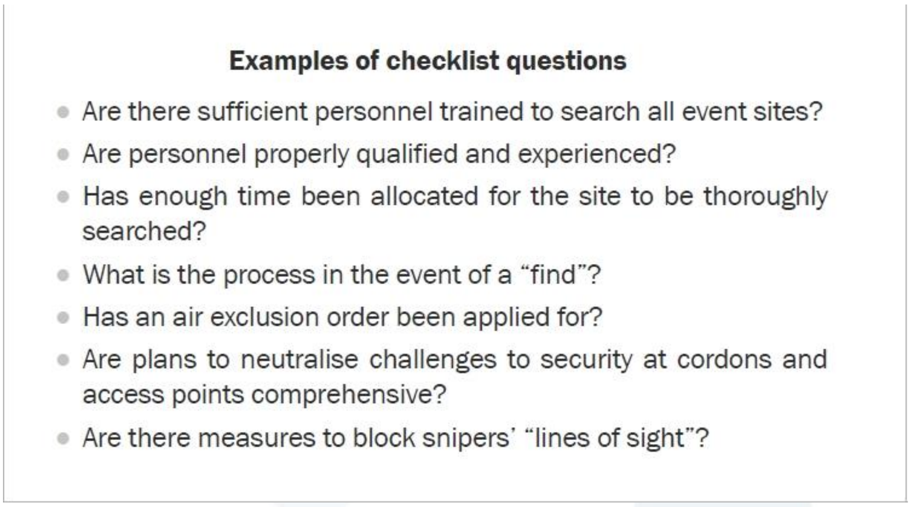
- Are there enough security layers, rings and zones to protect the venue?
- Would the physical and non-physical barriers stop attacks by identifying threats?
- Is the buffer zone area sufficient to protect the inner area from the effects of a bomb attacks etc. on the outer cordon?
- Are personnel on 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[37]

- **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

[37] Checklist pointed out in UNICRI (2007), IPO Security Planning Model

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.[38]



**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”?

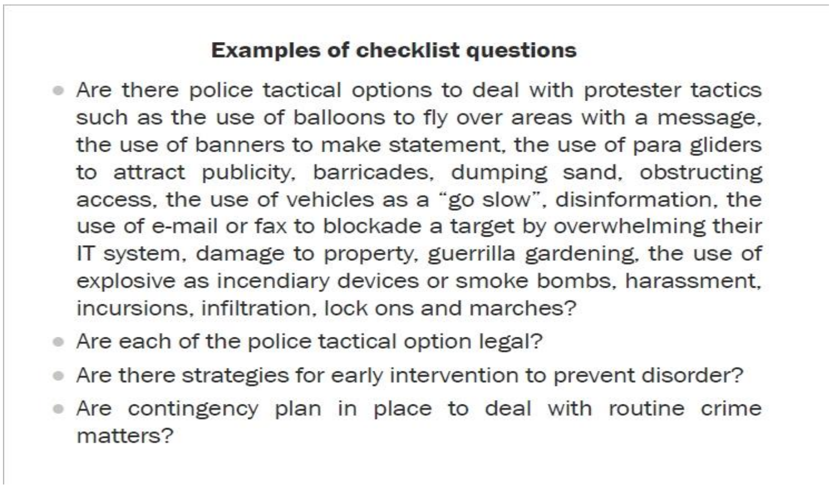
**Checklist 2 Search, seal, secure and keep secure[39]**

- **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. For helping this proactive engagement the Letscrowd server has an online message tool used for sending text and multimedia information. LEAs 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.[40]

[38] UNICRI (2007), IPO Security Planning Model

[39] Checklist pointed out in UNICRI (2007), IPO Security Planning Model

[40] UNICRI (2007), IPO Security Planning Model

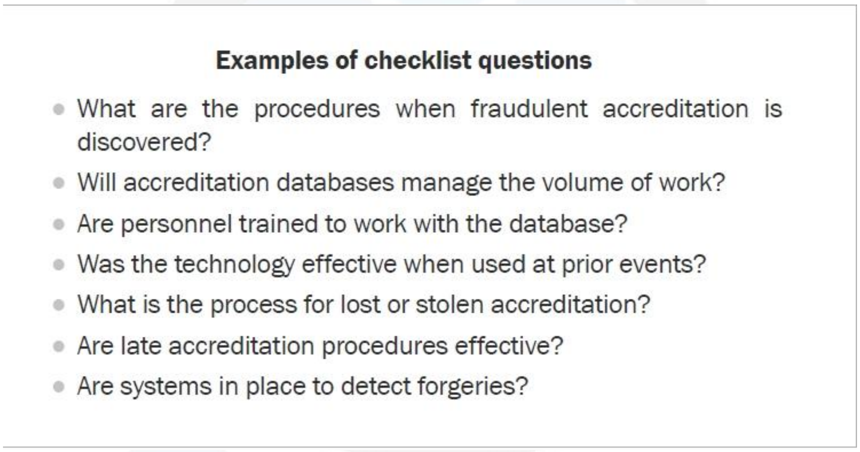


**Examples of checklist questions**

- 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[41]

- **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.[42]



**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[43]

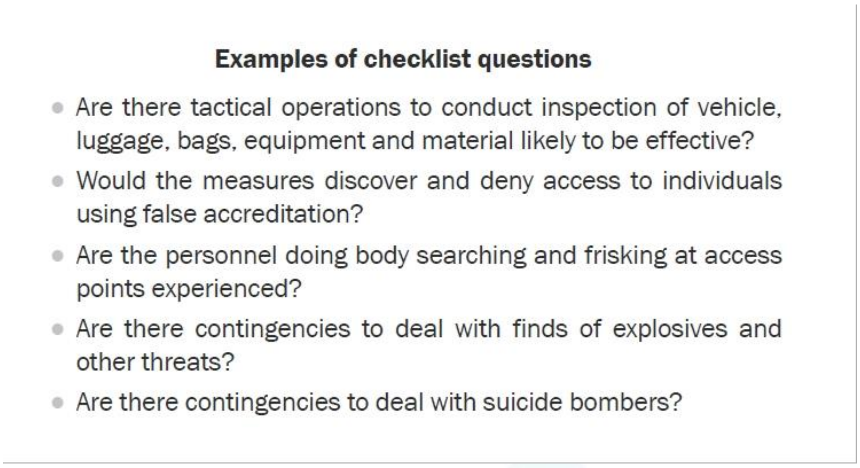
- **Access Control:** Identifying venue access and egress points for different categories of persons, including principles delegates, media, participants, spectators, etc., to control entry and deny access to unauthorized people, those with prohibited items, and anyone else prohibited from entering for 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.[44]

[41] Checklist pointed out in UNICRI (2007), IPO Security Planning Model

[42] UNICRI (2007), IPO Security Planning Model

[43] Checklist pointed out in UNICRI (2007), IPO Security Planning Model

[44] UNICRI (2007), IPO Security Planning Model

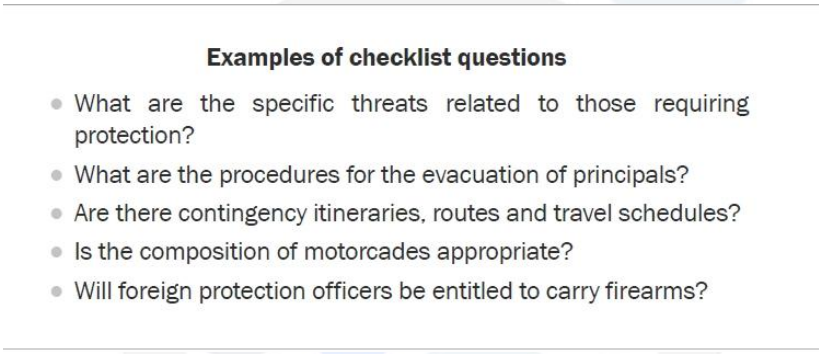


**Examples of checklist questions**

- 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[45]

- **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.[46]



**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[47]

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

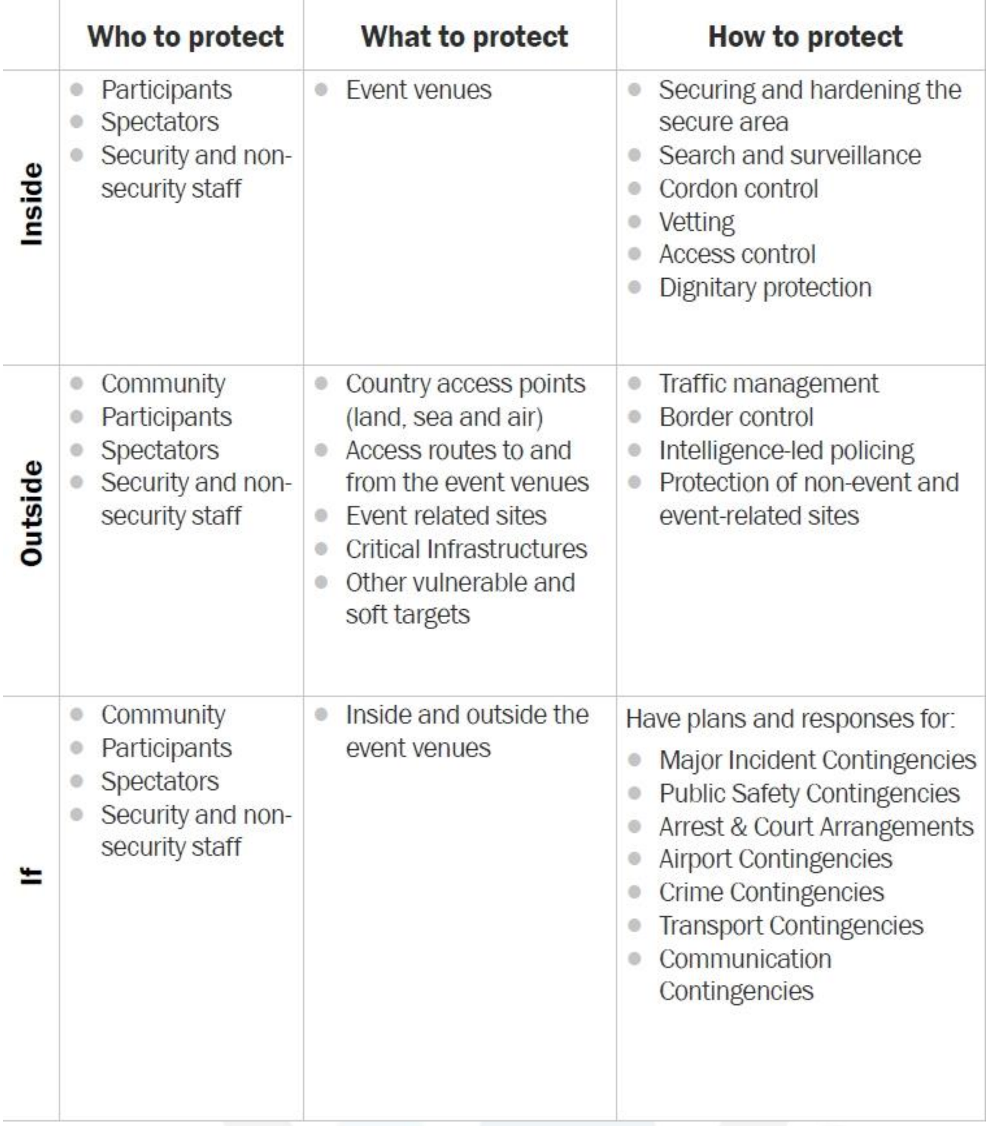
- Save life, protect property and prevent crime inside the designated secure area (inside),
- Save life, protect property and prevent crime outside the designated secure area (outside),
- To be prepared in security related contingency planning terms (if).

Figure  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.

[45] Checklist pointed out in UNICRI (2007), IPO Security Planning Model

[46] UNICRI (2007), IPO Security Planning Model

[47] Checklist pointed out in UNICRI (2007), IPO Security Planning Model



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

Figure 3[48] - Security plans for venues (Who, what and how; inside, outside, if)

Within the normal course of designing a security plan, it is imperative to recognise the importance of developing a broad view of proactive and preventive measures that can and should be used in collaboration with physical security measures. This comprehensive outlook must reflect the nature of any potential threat so that it can be recognised, foreseen and clogged before striking the potential target(s).

## 4.6 BORDER CONTROL

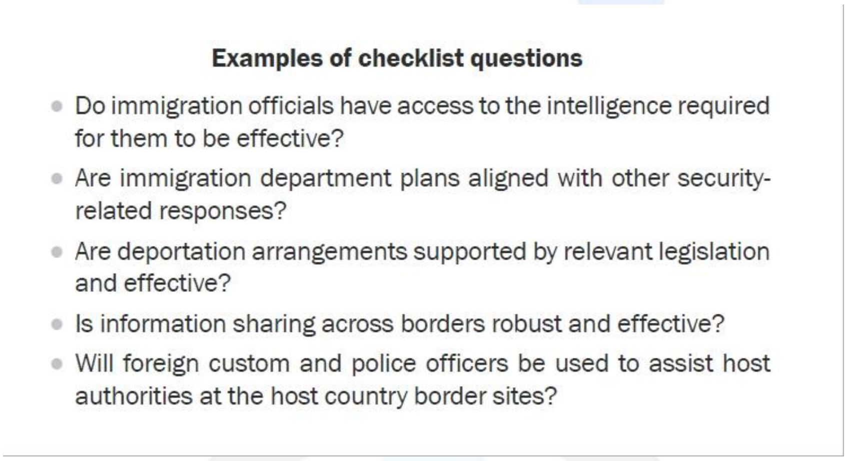
During the designated period of a major event, consideration could be given to strengthening routine border control activities to:

- 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.

[48] Figure used in UNICRI (2007), IPO Security Planning Model

- 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.[49]

This border control it's very common in major sports events. In practice, the lists of banning orders of the country of origin are communicated to the host country, and the assumptions underlying its issuance are equally applied. At the same time, considering that there is an effort to identify risk supporters, an agreement is reached between the national football information points and border control it's also carried out.



**Examples of checklist questions**

- Do immigration officials have access to the intelligence required for them to be effective?
- Are immigration department plans aligned with other security-related responses?
- Are deportation arrangements supported by relevant legislation and effective?
- Is information sharing across borders robust and effective?
- Will foreign custom and police officers be used to assist host authorities at the host country border sites?

**Checklist 7 Border Control**[50]

## 4.7 TRAFFIC MANAGEMENT

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

(a) 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.

(b) 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.

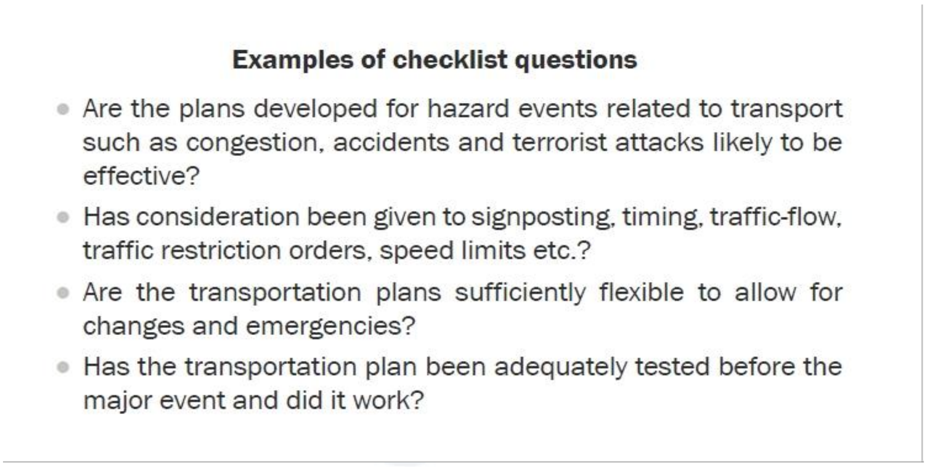
(c) Project a public transportation system that is capable of handling expected volumes of people at given times and places in a safe and secure way.

(d) 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.[51]

[49] UNICRI (2007), IPO Security Planning Model

[50] Checklist pointed out in UNICRI (2007), IPO Security Planning Model

[51] UNICRI (2007), 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[52]

## 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 non-event sites such as critical infrastructures, normally settled by law and soft targets[53][54].

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

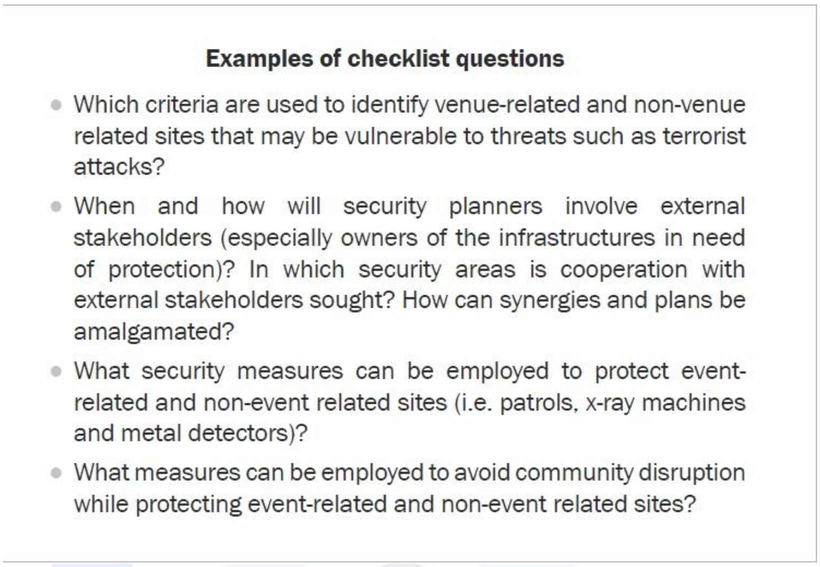
- **Assessment:** Identification of those event-related and non-event related infrastructures and assets that could become vulnerable during the major event in terms of national-level public safety and security.
- **Awareness:** Promotion of awareness amongst all stakeholders of the potential for and 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.[55]

[52] Checklist pointed out in UNICRI (2007), IPO Security Planning Model

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

[54] 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.

[55] UNICRI (2007), IPO Security Planning Model



**Examples of checklist questions**

- Which criteria are used to identify venue-related and non-venue related sites that may be vulnerable to threats such as terrorist attacks?
- When and how will security planners involve external stakeholders (especially owners of the infrastructures in need of protection)? In which security areas is cooperation with external stakeholders sought? How can synergies and plans be amalgamated?
- What security measures can be employed to protect event-related and non-event related sites (i.e. patrols, x-ray machines and metal detectors)?
- What measures can be employed to avoid community disruption while protecting event-related and non-event related sites?

Checklist 9 Non Event and Event Related Security[56]

Therefore, Planners should consider:

(a) Identifying the vulnerable non-venue and event-related elements that if attacked would have significant impact on public safety, health, governance, the economy and/or national security.
(b) Promoting stakeholder awareness of the realistic potential for attack and seek support and shared responsibility in terms of implementing effective crime prevention measures.
(c) Designing early warning mechanisms for attacks against identified non-venue and event-related sites and graded response options thereto.

## 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.[57]

There’s no doubt that the complexity of planning implies vigorous and dedicated provision specially in respect of matters such as financial management, project management, staff selection, tasking & coordinating, meeting & correspondence management, the preparation of timelines & Gantt charts, legal research, health & safety and project administration.

[56] Checklist pointed out in UNICRI (2007), IPO Security Planning Model

[57] UNICRI (2007), IPO Security Planning Model

To plan effectively security planners need to be experienced and professional and, in terms of the event related resources operationally deployed, personnel should be adequately trained, equipped and briefed.

Different skills are required ranging from the ability to deal with protester tactics, CBRN responses and media support. Needless to say, capacity requires careful management. Depending upon the scale of the event, some of the personnel may have secondary function to fulfil that could absorb them from their event related tasks. In this respect, there should be no misapprehension about the tasks and duties that officers are expected to perform.

Some authorities consider it good practice to issue a directive restricting leave to ensure, firstly, that the requisite number of officers needed for event related functions are available and, secondly, that sufficient officers are still available to perform routine community-based policing activities.

Security planners also need to consider the provision of adequate logistical support in terms of matters such as catering, accommodation and transport. Enhancing the human aspects of the response with reliable equipment and technological solutions such as CCTV, sensors, detectors and means of communications is important.

The nature and the extent of the event will direct the levels of technical support required to enhance security but, given the extensive range of communication and IT equipment available, the very high costs involved, the rapidly changing market and the level of skill required to properly establish the most applicable solutions, it is recommended that each event is considered on an individual basis and, with professional support, that only the most appropriate solution is sourced.[58]

## 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.
- 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.[59]

About communication services used during a major event, it’s capital to guarantee:

- Radio Interoperability - For some special events, the lead agency may be able to disseminate radios on the same frequencies to all personnel involved in security. More commonly, other approaches are used to enable personnel from multiple agencies (with different radio models operating on different frequencies) to communicate in the field. The lead agency may use advanced communications technology to link radios with different frequencies into a common communications matrix. This evolving technology acts as a networking gateway that interconnects radios with any frequencies into a common event frequency. Thus, one very important principle in security planning for major special events is to create policies and procedures for all partners, governing officials, private security, and others to communicate regularly on event planning and

[58] Conners, E. (2007). Planning and Managing Security for Major Special Events: Guidelines for Law Enforcement. Institute for Law and Justice

[59] UNICRI (2007), IPO Security Planning Model

management. All parties should use e-mail, with its distribution list and storage capabilities, extensively to keep all partners up-to-date and informed on plans, decisions, agreements, issues, and more.

- Integrated Communications Command Centre - One of the most important components in planning security for major special events is to develop an integrated communications command centre. The integrated communications command centre brings together key leaders and actors from all the agencies and jurisdictions involved in supporting security at the event. The Integration Centre is in the process of developing standards, guidelines, protocols, and more to support incident management response development at the state and local level. In developing an integrated communications command centre for a special event, the centre should be able to access and observe the routine calls for service that are being dispatched on the local law enforcement's computer-assisted dispatch system. The terminal should be located, along with an experienced dispatcher, in the command centre. The command centre should also know about routine police calls that are occurring throughout the city that could possibly have some relationship to event security.[60]

## 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 if equipment is appropriate.[61]

Coordination and the development of procedures is a major undertaking because of the high number of stakeholders involved at so many different levels. Many are often not used to working together toward a common goal. Coordination involves three principles:

- The first principle is that every individual of every organisation involved should understand their specific role in the wider organisation of the major event and should be able to act accordingly. The individual members of the larger organisational system – the venue steward, the police officer on the street, the staff member at the media park – have to be briefed on what they need to know. The principle here is to "keep it simple", the simpler the plan, the better.
- Secondly, during the preparations one should take special care of "planning the plan". Agencies are expected to develop their own plans to be able to perform their task during a major event. Most major events are like giant jigsaw puzzles where many agencies have different roles. Care has to be taken in respect of problems that can arise as a result of concurrent and parallel planning. When plans are not matched, misunderstandings can seriously undermine the overall operation.
- Thirdly, the best test of procedures and planning is practice. Procedures should be shown to work in real-time and be effective on site. Thus, special consideration should be given to how coordination will work during the event itself.

The following factors may present obstacle coordination:

- Local, national and international stakeholder issues.
- Who pays for what.

[60] Conners, E. (2007). Planning and Managing Security for Major Special Events: Guidelines for Law Enforcement. Institute for Law and Justice

[61] UNICRI (2007), IPO Security Planning Model

- Jurisdictional disputes.
- Organisational culture and conflict.
- Independent action outwit the agreed plan.

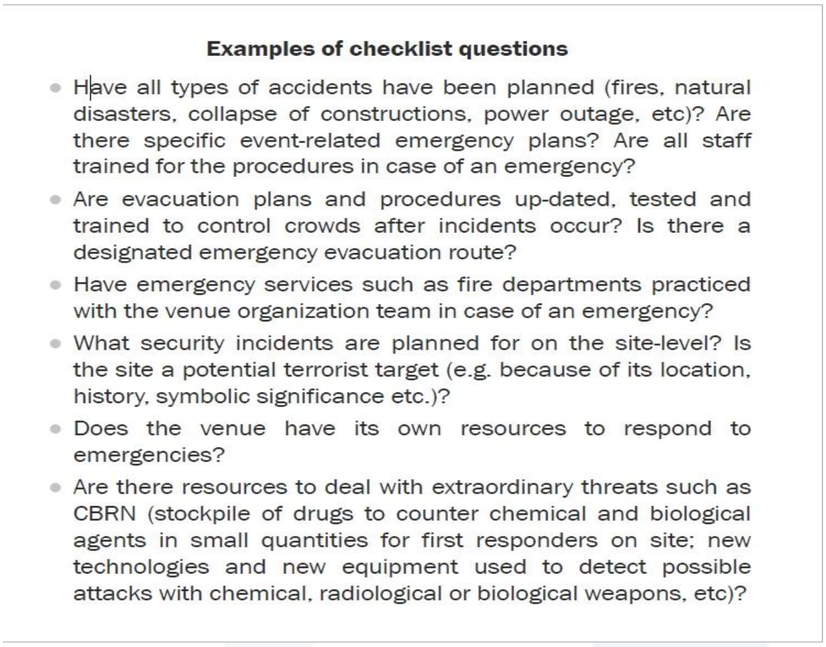
Coordination is needed to bridge gaps between plans and practice.

## 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.
    - Restoring normality as soon as possible.
    - Ensuring scenes and evidence are preserved.
    - Facilitating investigations and inquiries.
    - 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.[62]

[62] UNICRI (2007), IPO Security Planning Model



**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**[63]

[63] Checklist pointed out in UNICRI (2007), 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 second version of a total of 2 deliverables that address security policy specification.

As discriminated in the Scope of this deliverable, the D4.3 was related to the methodologies used by the PSP, specifically regarding the decision-making process, planning and risk analysis in the management of major events, presenting the main lines used.

At the time of production of the first version, we proposed to carry out a subsequent analysis of the guidelines used by the remaining LEA partners of the project. Subsequently, it was concluded that only PSP has national responsibilities in this area, and the other partners have a municipal or regional character, and some of them have no public order competences.

In this perspective we have pointed out our efforts for the Europe, and it was possible to conclude that, like Portugal, a substantial part of the European countries also assumed the premises of the IPO Security Planning Model and later in the EU-SEC, considering that they participated in its elaboration. It should be noted that the 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 and the Netherlands United Kingdom. Funded by the European Commission, the EU-SEC Project aimed at co-ordinating national research programs on security of major EU events in Europe.

In fact, the IPO programme presents its ‘Security Planning Model’ to further the international identification and exchange of good practices, representing a common framework to link national approaches to the security planning of major events, covering the areas that the IPO programme and its experts, with the allowance of a few European countries, already named, have considered most relevant and pressing nowadays, but never without considering that in addition to a plethora of universal concerns, policy makers and planners also have to contend with issues specific to the host country and the event taking place, which the ‘Security Planning Model’ leaves room for. To this end, it poses questions that it feels policymakers and planners who are called upon to elaborate, develop and implement security programmes needed to host a safe and secure major event should aim to answer.

For those reasons we have decided to complement the work presented in the first version, using the same structure and topics carried out, special the ones that we have considered to be the key points for security policy specification guidelines, bestowing at the end:

- The decision process
- How should be planed the covering of a mass gathered event
- Which are they key aspects for planning pre-event, event and post-event execution phases
- How is normally calculate the risks and how do the risk and the INTELPOL will affect the decision that has to be made
- The importance of information exchange between the different countries of EU in order to minimize worldwide threats during a Major Event
- Which are the guidelines for security policy specification adopted by a significant number of countries in Europe.

# 6 References and Acronyms

## 6.1 REFERENCES

1. BAS, E. (2010). Prospectiva – Cómo usar el pensamento sobre el futuro. Barcelona: Editorial Ariel, S.A.

*2.* CLARK, R. (2010). Intelligence Analysis: A Target-Centric Approach (3ª Edição). Washington: CQ Press.

3. Conners, E. (2007). Planning and Managing Security for Major Special Events: Guidelines for Law Enforcement. Institute for Law and Justice

4. Cuesta, J.H. & Jarvis, N. (2004). IPO Closed-Door Meeting, Madrid.

5. FERNANDES, L. (2014). Intelligence e Segurança Interna. Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna.

6. GRABO, C. (2010). Handbook of Warning Intelligence – Assessing the Threat to National Security. Plymouth: Scarecrow Press, Inc.

7. GREENE, J. et al. (2002), Safety and security at the Olympic Games in Salt Lake City, Utah. Washington, D.C., Bureau of Justice Assistance, U.S. Department of Justice.

8. HEUER, R. e PHERSON, R. (2011): Structured Analytic Techniques for Intelligence Analysis. Washington: CQ Press.

9. ISO 31000 – Risk management – Principles and guidelines.

10. LINDGREN, M. e BANDHOLD, H. (2003). Scenario Planning: The link between future and strategy. Nova Iorque: Palgrave Macmillan.

11. NCS, (2017). Project STADIA. Sports security Senior Management Training Course

12. Project, EU-SEC. *Website.*

13. *SCHWENKER, B. e WULF, T. (Eds) (2013). Scenario-based Strategic Planning: Developing Strategies in an Uncertain World. Munique: Springer Gable.*

14. TORRES, J. (2015a). A Gestão contingencial de cenários de risco para a segurança pública. In: Valente, M. (Coord.). Ciências Policiais e Política Criminal (pp.141-165). Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna.

15. TORRES, J. (2015b). Gestão de Riscos no Planeamento, Execução e Auditoria de Segurança. Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna.

16. *UNICRI (2007). IPO Security Planning Model.*

17. WATSON, R. e FREEMAN, O. (2012). Futurevision: scenarios for the world in 2040. Melbourne/Londres: Scribe Publications.

18. WEICK, K. e SUTCLIFFE, K. (2007). Managing the Unexpected: Resilient Performance in an Age of Uncertainty (2ª Edição). São Francisco: John Wiley & Sons, Inc.

## 6.2 ACRONYMS

| Acronyms List | |
|---|---|
| LEA | Law enforcement agency |
| 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 |
| UNICRI | United Nations Interregional Crime and Justice Research Institute |

Table 1 Acronyms