unicri

advancing security, serving justice,
building peace

IPO
Security Planning Model

2007

INTERNATIONAL PERMANENT OBSERVATORY ON
SECURITY DURING MAJOR EVENTS IPO

The IPO
Security Planning Model

Foreword

Hosting worldwide major events has a long-standing tradition but much has changed over the years. What were once major exhibitions of technological advancement are now a regular aspect of international life, providing a platform for all kinds of global achievements be they athletic, religious, technological, cultural or political. Such events like the Olympics, vibrant national Festivals and influential G8 or WTO summits involve not only the hosting organization, nation or government and participants but also the surrounding community and global viewers. The impact of global events has undoubtedly expanded, so our attention to it must develop with similar momentum.

The knowledge, practices and guidelines of international bodies to help states to host secure major events have not developed rapidly enough. One need only remember the tragedies during Munich 1972 Olympics and Atlanta 1996 Olympics to realise that major events drastically increase the risk of terrorist attacks. Major events unfortunately provide high visibility, public attention, a dense concentration of individuals, the presence of VIPs media coverage that perpetrators of organised crime, common criminals and radical activists can exploit. The threat that terrorism poses on daily security is already substantial as seen with the attacks of September 2001, the Madrid bombings of March 2004 and the London suicide attacks of July 2005. Given the increased vulnerability of major events, more so than the already significant day-to-day threats, the security planning and international exchange of best practices for major events needs to more advanced than ever before.

For this reason, The United Nations Interregional Crime and Justice Research Institute (UNICRI) has addressed the issues associated with the security during large events by launching the International Permanent Observatory (IPO) on Security Measures during Major Events in 2003. IPO is the first worldwide mentoring service created specifically to enhance the capability of national authorities to maintain security during major events, promote international cooperation in the field, and to bring together experts from national public authorities whose core business involves security. The IPO network consists of internationally recognised experts with varied backgrounds in the fields of security, and provides a forum with useful information for these experts. The IPO was formally acknowledged for its efforts by the ECOSOC Resolution E/2006/28 of July 2006. Fostering international cooperation before, during and after a major event will provide added security where, we feel, it is needed most.

The IPO programme presents its ‘Security Planning Model’ to further the international identification and exchange of good practices. It is a common framework to unite national approaches to the security planning of major events. It aims to cover the areas that the IPO programme and its experts consider most relevant and pressing in our current era. 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. UNICRI here contributes a valuable and useful resource to any requesting Member-State to further the international community’s progression towards a more safe and secure world.

Sandro Calvani
Director of UNICRI

Acknowledgements

The preparation of the IPO Security Planning Model benefited from the input of many individuals, institutions and organisations that provided precious contributions since the launch of the International Permanent Observatory on Security Measures during Major Events in 2003.

UNICRI is grateful to all the experts who shared their knowledge on security issues during the seven Closed-Door Meetings organised within the framework of IPO and to their respective institutions for ensuring their attendance.

UNICRI is particularly grateful to the UNICRI Senior Fellows and IPO staff, Mr. Francesco Marelli and Mr. Brian Powrie, for having drafted the document.

A special thank you should also go to Ms. Doris Buddenberg, who constantly provided encouragement to IPO while she was UNICRI Acting Director. Special acknowledgement should also go to Mr. Francesco Cappé, who coordinates UNICRI's activities in the field of Security Governance and Counter-Terrorism, and to IPO staff, Mr. Massimiliano Montanari and Mr. Alberto Pietro Contaretti, who played a major part in the development of IPO. UNICRI's gratitude also goes to Marc Otten, a UNICRI's Consultant, who drafted the *Toolkit for Policymakers and Security Planners*.

UNICRI is grateful to the European Police Office (EUROPOL) for the technical support they have provided since the launch of IPO and for the insightful comments and contributions offered by its officers during the preparation of the IPO Security Planning Model.

Special acknowledgement should also go to the Chairman of the IPO Advisory Committee, General Ma Zhen Chuan, Director General of Beijing Public Security Bureau of People's Republic of China, and to the Members of IPO Advisory Committee: Mr. Sergey Girko, Head of the All-Russian Research Institute of the Ministry of Interior of Russian Federation, Mr. Domenico Paterna, Colonel of the Italian Carabinieri Corps, Mr. Arne Huuse, Police Commissioner, National Police Directorate of Norway, Ms. Ann Brooks, former Director of the Special Events Office of the US Department of Defence and Mr. Juan Hidalgo Cuesta, former Advisor of the Secretary of State, Spanish Ministry of Interior, Secretariat for Security.

UNICRI wishes to underline the work done by the other IPO Staff, Ms. Houyam Boudiaf, Mr. Pavel Maximov for the layout and graphics, Ms. Laura Mitta, Ms. Annaclara Pochettino, Ms. Diane Raineri, Ms. Pimpernel Sieders and Mr. Shaoying Zhang for supporting the IPO activities.

Finally, UNICRI is deeply grateful to the Compagnia San Paolo whose financial contribution to IPO's activities made it possible to develop this IPO Security Planning Model.

List of contents

Introduction 1

1 **The International Permanent Observatory (IPO)** 3

2 **The IPO Security Planning Model** 7

2.1 Definition of Major Events 7

2.2 The main elements of major event security planning 9

2.3 The IPO Security Planning Model 17

2.4 Planning Response Continuum 20

2.5 Assimilation 21

2.6 Conclusion 23

3 **The System** 25

3.1 Governance 25

3.2 Capacity 32

3.3 Constraints 37

3.4 Intelligence 42

4 **The Deliverables** 47

4.1 Plans inside the designated secure area 48

4.2 Plans outside the designated secure area 53

4.3 Contingency Plans 57

5 **The Risks** 61

6 **IPO Assistance** 65

Introduction

The occurrence of a major event 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.

Such a concise introduction does little to convey the complexity and the scale of planning security required for a major event but this IPO Security Planning Model is not intended to complicate the subject any more than is necessary.

Designed as an instrument to assist national authorities, this publication provides a pragmatic and sensible planning framework that identifies, describes and simplifies the main tools that policymakers and security planners have used to plan and implement security at major events in the past. It provides an introduction to the main planning considerations and explains why security planning will become an exceptional undertaking. It also comprehensively highlights the strategies, questions, linkages and other challenges that security planners should take into account. The IPO Security Planning Model is available to public bodies responsible for, or otherwise involved in, planning the provision of security at a major event. The document is grounded on international experience and best practice gathered and collated by UNICRI.

The IPO Security Planning Model is divided into six chapters. The first introduces UNICRI's International Permanent Observatory Programme and its remit to share best practice and strengthen international cooperation in major event security matters. The second chapter explores how to define a major event and introduces a list of steps that policymakers and security planners should consider at the complex earlier stages of planning. This chapter concludes by offering a model that conceptualises these steps. The third, fourth and fifth chapters thereafter describe the main components of this model. Chapter six expands on how Member States can engage UNICRI and obtain, free of charge, IPO advisory services from a comprehensive menu of options.

Chapter 1

The International Permanent Observatory (IPO)

In 2003, the United Nations Interregional Crime and Justice Research Institute (UNICRI) launched the International Permanent Observatory (IPO), a global security and counter terrorism programme, designed around three main considerations.

The first consideration was that planning and implementing security for major events is a challenging exercise that should not be underestimated. The scale and complexity of planning an appropriate response to diminish potential risks will be extremely challenging. The cost, in both financial and staffing terms, will be very large. The event may involve several venues, in one or more cities with high population density, high levels of traffic and a range of vulnerable targets. The major event will also bring disruption to 'normal business', scrutiny and criticism from internal and external bodies, and significant pressure to satisfy the widest imaginable range of stakeholders. Moreover, large numbers of people and infrastructures will be exposed to different threats ranging from terrorism to hooliganism to natural disaster.

The second consideration was that a major event often offers the finance and the availability of resources to expand infrastructure, introduce systems and practices, procure equipment and expertise, develop training and expand capacity. All these elements help to instil more sustainable practices, ways of thinking and longer term security governance. In other words, the effective management of security at major events not only represents a crucial factor in the overall success of a world-class event, but also creates opportunities for an innovative, meaningful and lasting security governance legacy.

The third consideration was that the knowledge and expertise necessary to successfully deal with major event security are not easily accessible and there is neither a blueprint nor an international security manual applicable to any kind of major event. Policies, strategies and tactical operations need to be adapted to current threat levels, human resource capacity and technological solutions available, local legislative conditions, political aspirations and a range of other crucial factors. Plans need to be developed flexible enough to cater for the inevitable changes that will almost certainly emerge prior to, during and even after the event.

Starting from these three considerations, UNICRI designed IPO as a body of experts whose specific purpose is to collect knowledge and expertise from past major events, absorb and incorporate lessons learnt, and deliver them through user-friendly formats and tools to requesting national authorities.

The **collection of knowledge** through closed-door meetings is a central aspect of the Observatory and involves experts, with first-hand experience in organising different types of major events, sharing their knowledge. Addressing specific security related topics, these meetings helped IPO bring together a bulk of knowledge and good practice regarding the security of major events. Alongside these meetings, IPO developed a **Restricted Documentation Centre (RDC)** that stores a wealth of important information on security at major events in the form of event security plans, event after action reports, technical reports, threat assessments and other documentation.[1]

Equally important is the **analysis** through which IPO identifies the main elements that security planners should take into consideration whilst planning security of major events. Along with this IPO Security Planning Model, IPO has produced a **Toolkit for Policymakers and Security Planners** and regularly develops **Ad Hoc Planning Guides for Major Event Security**. It will be a comprehensive reference document on planning, operational implementation and post event activity.

Finally, IPO offers major event security planners, upon request, a range of **mentoring and quality-assurance services** by drawing upon the expertise of a global bank of experts, all of whom have held key security positions at past major events. The expertise of these officials is donated by law enforcement and security agencies of different United Nations Member States as an in-kind contribution to the programme. UNICRI also enjoys the individual support of security experts who are part of the established IPO network.

Acknowledging the importance and value of the IPO Programme, in July 2006 the Economic and Social Council of the United Nations (ECOSOC) approved Resolution E/2006/28 on IPO. In this resolution, ECOSOC

[1] Access to the Documentation Centre may be permitted, upon request, to public authorities responsible for, or otherwise involved in, planning the security of a major event. For more information see IPO website: www.unicri-ipo.org.

encourages Member States planning major events to take advantage of IPO in order to receive information on best security practices in relation to major events and invites UNICRI to continue and expand its work on the Observatory, including the provision of technical assistance and advisory services on security during major events to Member States upon request.

Furthermore, the Handbook for Crisis Prevention and Response at Major Special Events, produced by the G8 Lyon-Roma/Anti-Crime and Terrorism Group and the Law Enforcement Projects Subgroup (LEPSG), explicitly encourages the utilisation of the IPO platform.

Chapter 2

The IPO Security Planning Model

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 major event security is largely about coping with complexity.

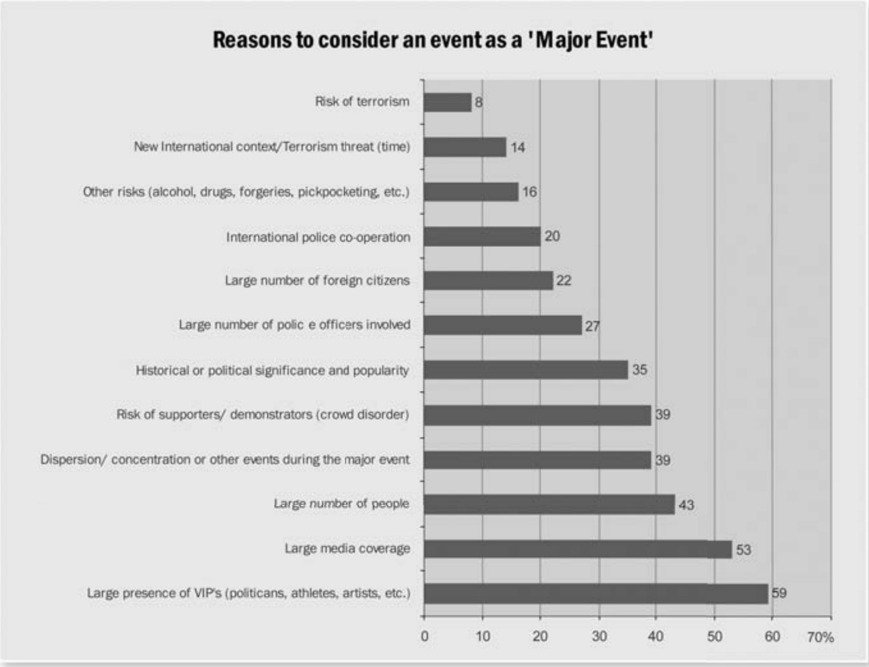
This chapter introduces the IPO Security Planning Model which articulates and makes much more transparent the main components of the planning process and the guiding principles that underpin the provision of security at major events.

2.1 Definition of Major Events

Given the absence of a universally accepted definition, IPO engaged the assistance of international experts and participants in the project Coordinating National Research Programmes on Security during Major Events in Europe (EU-SEC) to try and define what constitutes a major event.[1] To explore the concept, participating countries offered a great deal of detailed information about security measures that they designed and employed while hosting major events in the past. Overall, 30 major events were taken into consideration.

[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.

As shown in figure below, the participating countries identified a number of characteristics that identify major event, including:



A common definition of a major event was hence proposed by the EU-SEC project:

A **Major Event** can be defined as a foreseeable event that should have at least one of the following characteristics:

- 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 persons

and poses the potential of threats and therefore may require international cooperation and assistance.

Taking into account other factors, for instance the cost and the economic impact of a major event, what emerges from the work that has been carried out is that planning security for a major event is a very complex exercise that requires a range of measures and activities beyond those normally encountered.

2.2 The main elements of major event security planning

Due to their complexity, major events are likely to demand the creation of an **extraordinary and possibly temporary response.** Existing structures and procedures may not be sufficient and may even require the creation of a new organisational set-up, the planning of a wide range of tactical options to address problems that may affect the course of the event, the involvement of new staff and logistics, the coordination and amalgamation of different forces and other extraordinary efforts.

IPO has identified 12 main elements to try and help security planners develop an effective strategy when planning major event security. This IPO Security Planning Model has not been envisaged as a technical manual, but rather as a valid document to guide and support the management of major event security planning.

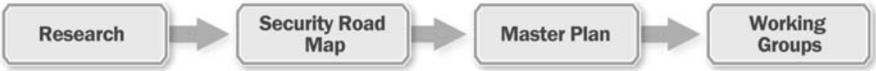
Element 1: Leadership

The appointment of a planning director, an individual with the leadership qualities, skills and experience required for planning and implementing security of the major event, is extremely important. Command protocols or contracts can articulate 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 formalised 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.

Element 2: Planning Structure and Management

The design of the planning structure is also important. This exercise could commence with research on the policing of previous major events from a critical perspective. The research may want to include, for instance, the identification of best practice for policing major events and an analysis of tactics used by protesters. After that, a planning director may want to identify and appoint a very limited number of senior planning staff members to conduct an exploratory but thorough scoping exercise to determine, as best they can, the extent of the operation. This exercise should help establish a broad concept of operations to start to transform a 'vision' into a meaningful, productive and cost effective planning structure. The team will seek to identify the main branches such as intelligence, venue security, traffic management, public order, logistics, human resources, command and control etc. These branches will make up the ultimate Master Plan.

Work within each branch could be supported by a working group. The leadership challenge is to ensure these branches, and the twigs that will emerge therefrom, are properly cultivated, trained, pruned and nurtured to ensure the growth is controlled to produce a tree that is of the right size, shape, form, appearance and strength.



Element 3: Intelligence

Inevitably, the structure will involve representations from a wide range of relevant agencies on local, national and international levels, all meaningfully contributing to a comprehensive intelligence system for gathering, analysing and disseminating intelligence and information to help security planners and others such as border control officials counter threats, vulnerabilities and risks. The system includes:

- 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 (**threat assessment**).
- The possible vulnerabilities of a target which could be exploited in an attack (**vulnerability assessment**).
- The likelihood or probability that potential threats will attempt an attack by exploiting the target's vulnerabilities (**risk assessment**).

There are various different information-based deployment systems to assist law enforcement operations. One such system is the UK's National Intelligence Model (NIM) that identifies patterns of crime and promotes a cooperative approach to problem solving.

The Handbook with recommendations for international police cooperation and measures to prevent and control and disturbances in connection with football matches with an international dimension, in which at least one Member State is involved publication promotes a model for intelligence-led cooperation and information sharing around events with an international dimension.[2]

Element 4: Media & PR Strategy

The external provision of coordinated, accurate and timely information is a very important element in any crime prevention or reduction strategy. It is essential to provide security related information and public reassurance, as well as to keep the media informed. Media monitoring is a key element as is the contingency planning of media responses in the event of any major incident. With this aim, it is important to:

- Design 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 etc.
- Offer public reassurance to explain to the community in simple terms why certain short-term restrictions may be necessary to deliver, for everyone involved, a safe and secure event. A number of instruments can assist this awareness campaign, including television programmes, information leaflets, banners etc.
- During the event, a robust media and PR strategy, executed effectively, provides a host of capacities, including opportunities to:
    - influence targeted audiences/stakeholders through the projection of specific messaging and the mitigation of misrepresentative or inaccurate reporting;

[2] The Council Resolution of 6 December 2001 adopted a first version of the Handbook (2002/C22/01).

- empower the organization(s) associated with major events/ activities to enhance or adjust stakeholder or targeted audience profiles through deliberate, planned communications delivered from recognized, trained and equipped sources;
- direct targeted audiences to respond in a certain way or adopt a specific posture in the event of a development requiring action;
- restrict rampant or alarmist communication, rumour or media reporting, or limit the impact thereof; and,
- contain, or more likely assist in containing, a situation through punctual communication of messaging in response to a specific development.

Element 5: Venue Security

The next step is to design the security plan for the controlled venue area and objectives of this step include:

- Identifying the designated secure area around the venue(s) and hardening that area with a range of human, physical and technical response options – **hardening the designated secure area**.
- 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) – **search, seal, secure and keep secure.**
- 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 – **public safety maintenance**.
- Designing systems to prevent infiltration of the venue event by persons who are not entitled to be there through a process of vetting, validation and accreditation – **vetting/ticketing**.
- Identifying venue access and egress points for different categories of persons, including principles delegates, media, participants, athletes, spectators etc., to control entry and deny access to unauthorised people, those with prohibited items such as drugs, weapons etc., and anyone else prohibited from entering for any other reasons – **access control**.

- Designing additional security arrangements for designated categories of participants such as dignitaries and VIPs etc. – **dignitary/personal protection**.

Element 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.

Element 7: Traffic Management

The main aims of this element are to:

- Maintain and secure access routes to and from venues and other designated places for delegates, media, police resources and others, which includes the management of road closures and other tactics involving for instance, the saturation and securing of critical and alternative routes.
- Maintain 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.
- Design a public transportation system that is capable of handling expected volumes of people at given times and places in a safe and secure way.
- Prepare 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.

Element 8: Non-Event and Event-Related Security

At this stage, security planners should consider extending 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 as hotels, sponsor villages, media centres etc, and critical infrastructures such as nuclear and chemical industry and installations, the utilities, communications and key transportation links. The protection of soft targets such as shopping centres, tourist sites and historical monuments should also be considered.

Planners should consider:

- 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.
- Promoting stakeholder awareness of the realistic potential for attack and seek support and shared responsibility in terms of implementing effective crime prevention measures.
- Designing early warning mechanisms for attacks against identified non-venue and event-related sites and graded response options thereto.

Element 9: Human Resources and Logistical Support

Having identified operational requirements, security planners have to consider populating security plans with human, physical and technological resources. Aims would include:

- Supporting 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.
- Providing 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.

Consideration also has to be given to plans for after the event to achieve:

- Planned withdrawal of personnel, equipment and security measures.
- Return to normality.

Clearly, the overall complexity of planning means robust and professional support must be considered in respect of matters such as financial management, project management, staff selection, tasking & coordinating, meeting & correspondence management, the preparation of timelines & gant charts, legal research, health & safety, project administration & clerical support.

Element 10: Information Technology (IT) and Communication

This step aims to establish communication strategies capable of satisfying the needs of the policing operation. Objectives include:

- **Communication and IT design**: establishing effective and hopefully secure radio, telephone and other means of communications to all organisations and agencies involved in the security of the major event, and other technological and IT solutions to enhance or support the human and physical elements of the plan.
- **Communication and IT controls**: ensuring that power supplies can be maintained, command centres and incident rooms are appropriately located, and that systems and IT security solutions are comprehensively tested prior to the event to ensure that everything is fit for purpose.
- **Communication and IT procedures**: establishing a clear framework of information flow procedures so that all actors involved will know who should inform whom of what and when. Consideration should also be given perhaps to the management of data produced by systems including elements such as CCTV product.
- **Communication and IT protection**: designing and implementing plans to protect core communication infrastructures and have prepared plans to maintain communications in case of emergency situations such as terrorist and protester attacks, accidents and natural disasters.

Element 11: Integration and Coordination

The next step involves an ongoing process to confirm that all the different branches of planning are integrated, complementary and coordinated. Aims are to:

- Test the integration, complementarity and flexibility of plans and their effectiveness (when and where they come together).
- Test the competence of the individuals and teams (who does what when and how).
- Test safety and security procedures to ensure they are aligned with standard operation procedures.
- Test equipment is fit for purpose against prevailing conditions.

Element 12: Contingency Planning and Crisis Management

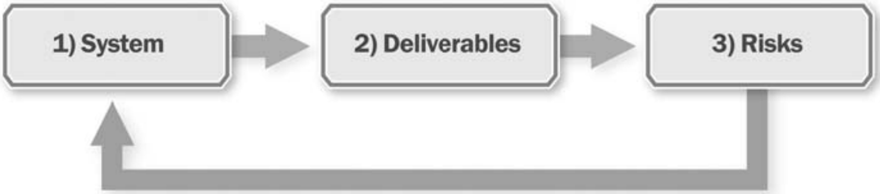
The consequences of an incident caused by terrorist attack, public disorder, natural disaster, accident, man-made emergencies or any other factor could be catastrophic and therefore it is necessary to develop contingency plan for such occurrences. Contingency plans are designed to assist in activities for:

- 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.

2.3 The IPO Security Planning Model

Having identified the main elements that security planners should consider while planning major event security, IPO would like to propose a pragmatic model that incorporates all these elements. The purpose of the model is not to teach planners how to plan. This IPO model offers a user-friendly structure that helps to identify the main components of the planning process and captures the main concepts that underpin each.

Starting with a very basic schematic representation, the model includes three main components: a **system** that produces **deliverables** to address existing and potential **risks**.

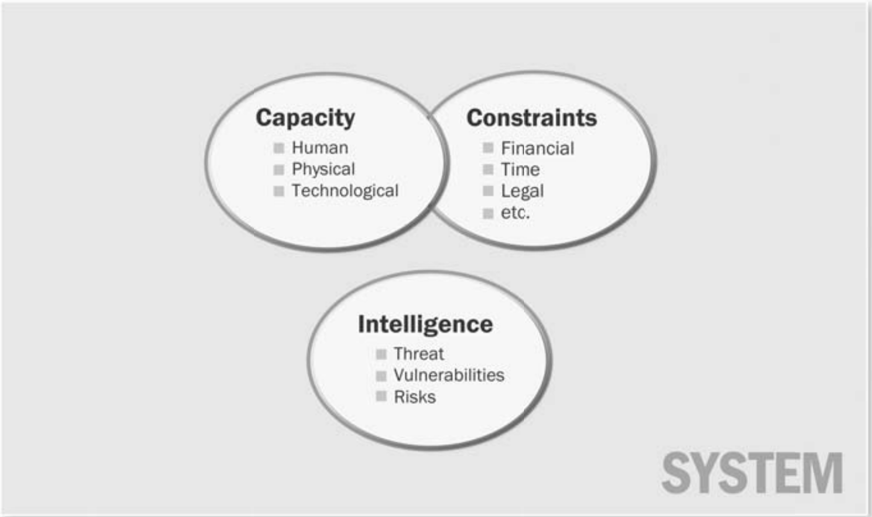


1. The System

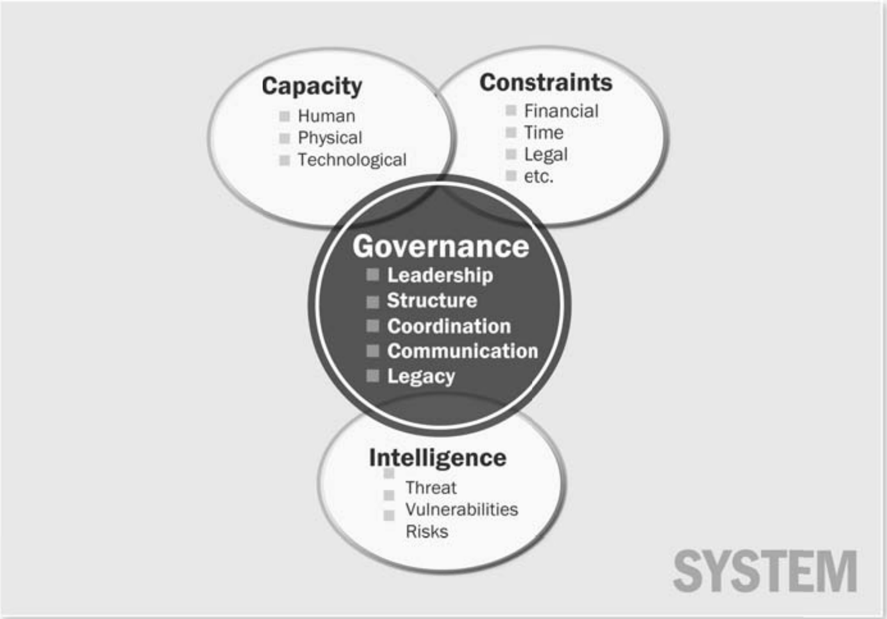
The **System** is an entity/organisation involving a group of people who are brought together for a common purpose. The System encompasses four main constituents: capacity, constraint, intelligence and governance.

As shown in the figure below, the first three are here considered:

- **Capacity** can be defined as the constituent that security planners have at their disposal in terms of human, physical and technological resources.
- **Constraints** can be defined as the quantifiable factors that restrict and regulate the extent of the capacity that can be applied. Constraints can include financial, time-related, legal, political and other factors.
- **Intelligence** describes the process of gathering and analysing information through which security planners can establish and thereafter design measures to diminish threats, vulnerabilities and risks identified.



Capacity, Constraints and Intelligence represent the "recipe's ingredients" that the system can bring together to create a product. The System, however, needs a "chef" and therefore the fourth key constituent for setting this strategic direction and delivering the product, i.e. the security plan, is Governance.



Governance can be defined as 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 heart of the organisation that leads, plans and implements effective, sensible and pragmatic security measures for major events.

2. The Deliverables

Deliverables make up the second component of the IPO model. They are the complementary plans and responses that the System designs and delivers to:

- 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**),
- be prepared in contingency planning terms (**if**).

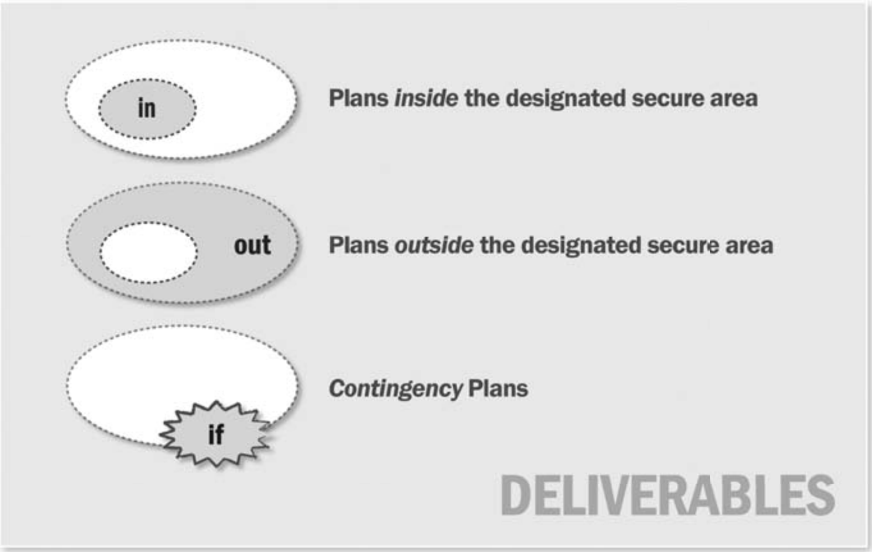
Inside: Plans inside a designated secure area should principally aim to protect:

- Participants: people taking part in the event and may include athletes, celebrities, politicians, etc.
- Spectators: people attending the event.
- Security and non-security staff: people working at the event including representatives from public and private organisations and agencies involved in the preparation, staging and delivery of the major event. This category includes sponsors, journalists and volunteers for instance.

Outside: Plans outside a designated secure area should principally aim to protect:

- Community
- Aforesaid Participants, Spectators and Staff when outside the designated secure area.

If: Contingency plans should aim to both counter emerging threats and have prepared a response if unexpected situations arise.


in
Plans *inside* the designated secure area
out
Plans *outside* the designated secure area
if
Contingency Plans
DELIVERABLES

3. The Risks

The third component of the IPO Security Planning Model is **Risk.** Risk is the presence of any element that may adversely challenge the security plan(s). Risks may arise:

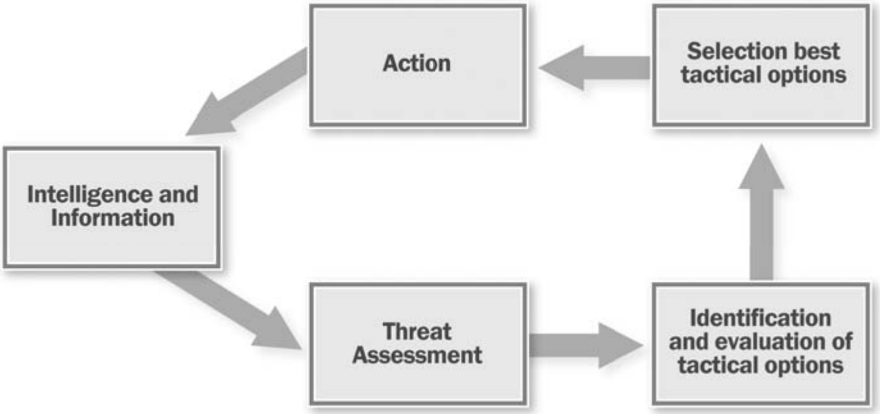
- From acts of **Terrorism**.
- **Public disorder** incidents.
- Occurrence of **Crime**.
- Acts designed to cause **embarrassment** such as media disclosures, single-issue demonstrations and staff strikes.
- **Accident, Emergency** and **Disaster**.

2.4 Planning Response Continuum

Planning and delivering major event security is a dynamic exercise in which strong leadership and effective management are required for optimal effectiveness. The process of planning and implementing security has an evolutionary and cyclical nature, characterised constantly by the formulation of detailed plans, the delivery of efficient solutions, the monitoring of day-to-day operations and an ongoing review.

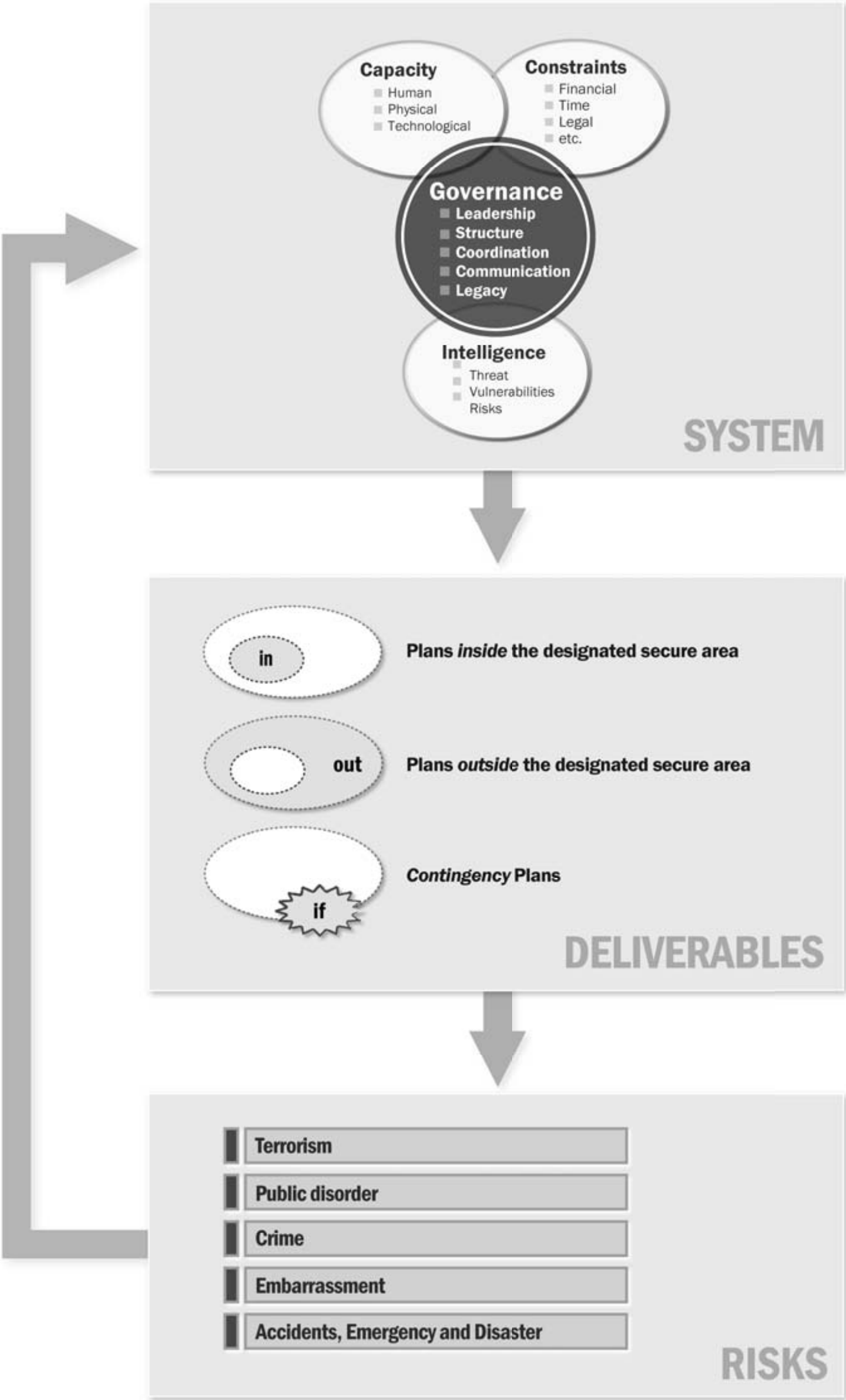
As shown in the figure below, at every stage in the process security commanders should consider:

- analysing all information and intelligence at their disposal to assess the risk
- their available capacity and quantifiable constraints
- identifying tactical options to diminish the assessed risk
- evaluating each tactical option to determine both advantages and disadvantages thereof
- selecting best tactical option(s), recording reasons for selecting these options and reasons for rejecting others
- introducing effective mechanisms for regular review


Action
Selection best tactical options
Intelligence and Information
Threat Assessment
Identification and evaluation of tactical options

2.5 Assimilation

Having broken down and examined the component parts (System, Deliverables and Risks), and introduced the concept of ongoing review, it is now possible, as shown in the figure below, to assimilate the IPO Model. It can now function as a guide for planners who, on the basis of available intelligence and information and working within quantifiable constraints and available capacity, want to develop a plan or set of complementary plans to effectively secure a major event.


Capacity
Human
Physical
Technological
Constraints
Financial
Time
Legal
etc.
Governance
Leadership
Structure
Coordination
Communication
Legacy
Intelligence
Threat
Vulnerabilities
Risks
SYSTEM
in
Plans *inside* the designated secure area
out
Plans *outside* the designated secure area
if
Contingency Plans
DELIVERABLES
Terrorism
Public disorder
Crime
Embarrassment
Accidents, Emergency and Disaster
RISKS

2.6 Conclusion

The occurrence of a major event is likely to demand the creation of 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 and property at both the event itself and within the community beyond, with contingencies prepared to counter emerging threats and respond when unexpected situations arise.

This chapter has introduced a number of elements, consideration of which will hopefully help planners get through the complex earlier stages of planning. A model that incorporates and conceptualises these elements has also been proposed. The next three chapters analyse the main components of the model.

Chapter 3

The System

Having introduced the IPO Model, this chapter now explores in more detail the first component thereof – the System – giving rise to the concepts of governance, capacity, constraints and intelligence.

3.1 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 encompasses five key concepts: leadership, structure, coordination, internal and external communication and legacy.

Leadership

Planning and implementing security for major events requires **robust leadership.** Working to a strict deadline, in a multi agency and often politically sensitive environment, with scarce resources, frequent interference, a limited budget and intense scrutiny throughout is not easy. Therefore, before any actual planning work commences, it is worthwhile to take the time to bilaterally negotiate, agree and formalise the appointment of an individual with the leadership qualities, skills and experience required for such a significant undertaking. Leaders will have to think long, hard and objectively about each element and evaluate each while taking into account the risks, threats and vulnerabilities of the event.

Major events require both leadership and management. Leadership is about establishing direction and developing a vision that aligns and inspires a group of people. Management is about implementing the vision and strategy provided by leaders, coordinating and staffing the tasks, handling day-to-day problems and monitoring results.

It is therefore important that governance brings together strategic, tactical and operational level commanders. **Strategic commanders** have responsibility and accountability for the operation. They formulate the overall strategy for policing the major event. They should be able to communicate effectively and energetically the vision and strategy to the whole staff. They should encourage staff to be resilient, motivated, coordinated and prepared to positively overcome hurdles should they arise. Strategic commanders should maintain a strategic overview and should 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** on the other hand are responsible for assessing all available information and intelligence, applying professional judgement, co-ordinating 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.

Structure

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 organisational 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. In the past, major event security operations have been organised and structured according to a decentralised model. Its philosophy was based on the absence of a central or unified command and control system. Each law enforcement agency performed its tasks autonomously, with minimal coordination with other agencies. This was, for example, the case in the Atlanta model for the 1996 Summer Olympic Games. However, more recently, for instance during the 2002 Winter Olympics in Salt Lake City, Utah, a different model was adopted. It was based on the creation of a coalition of the public safety agencies directly involved in the major event. In such a case, while a single agency takes the lead in terms of coordination, others perform their roles according to an agreed framework.

Inclusiveness is important. Effective management and co-ordination of resources relies on the involvement of more than just one agency and could, for instance, include different police bodies (such as 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 and others. It is also advisable to start early interaction and cooperation with all other stakeholders not only during the implementation stage, but also during the planning phase. This would include the **community** whose protection is likely to be one of the main aims of the major event security plan. It is important to inform the community about what to expect, especially in terms of disruption to normal day-to-day routine. By establishing a good, frank and honest dialogue with the community it is much more likely they will support and understand especially when problems will arise. Another important category of stakeholder is the **business sector**. This sector is likely to need support in terms of developing contingency plans to protect their business activities from any type of attack or disruption.

Given the breadth of internal and external stakeholder involvement, the use of explicit agreements or memoranda of understanding may want to be considered.[1] **Command protocols or contracts** articulate exactly who has responsibility for planning and delivering what, where and when.

Effective command also relies on the principle of **flexibility**. There is not a universal planning structure ‘template’. Major events differ significantly from time to time and place to place as the event programme changes, different threats requiring different responses emerge, staff ‘contracts’ and conditions of employment vary, new or improved technological solutions become available, local legislative conditions and political aspirations apply and different venues inevitably present different challenges in terms of their physical security requirements. Security planning for a major event in a city for instance will be somewhat different to one taking place in a rural environment and this will be reflected in the eventual composition of the planning team and the structure that is applied. Within the normal course of developing a security

[1] This was one of the main themes of the IPO Closed-Door Meeting, Svalbaard, Norway, 2004.

concept of operations for a large event, it is imperative that all commanders recognise the importance of flexibility whilst deploying resources to identify, anticipate and stop potential threats.

Coordination

Co-ordination 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.
- Jurisdictional disputes.
- Organisational culture and conflict.
- Independent action outwith the agreed plan.

Duplication, overlap, redundancy, miscommunication and misunderstanding are features that can arise. Coordination is needed to bridge gaps between plans and practice.

Communication

Another important aspect of governance is internal and external communication. Effective **internal communication** within and across organisations and agencies involved in the security of the major event is paramount and a key element in coordination. It allows authorities to disperse information, keep everyone up to date and help in terms of understanding what is expected in operational terms.

External communication is also very important. Major events attract a great deal of media attention, some of it not entirely complementary. An effective external communication strategy has the potential to enhance public confidence and minimise potential harm to the reputation of the event security organisers. Elements of a communication strategy can be designed to:

- Create a positive public image for the event.
- Reassure the public about the extent of the operation and communicate information such as traffic and travel disruption, ticketing arrangements, travel options, recommended routes, location of facilities, and others.
- Keep the media appropriately informed.
- Monitor international, national and local media reporting.
- Develop strategies to ensure fair and accurate reporting.
- Develop policies and procedures for managing all official responses to media comments on major event security.
- Coordinate and facilitate press conferences on security.

Legacy

Governance is also about having the ability to create and articulate a realistic, credible and attractive vision of the future of the organisation. By inculcating legacy into major event planning from the start, by creating a planning culture and climate that seeks to derive longer term, tangible and meaningful benefits, by introducing an element of creativity and resourcefulness, by acknowledging and maybe even rewarding good ideas and, most importantly, by remaining objective, professional and pragmatic throughout, overall costs can be reduced and significant, long term and sustainable benefits can be amassed.

Legacy benefits and rewards can be counted in so much more than just simple financial terms. There are many ways to accrue legacy.

- **Community Trust, Respect and Confidence**: Major events are an excellent opportunity for police to gain and enhance the trust, respect and confidence of the community they serve. It is important from day one to engage the people that the police have to protect, serve, reassure and work alongside, particularly the elderly, the young and other vulnerable groups. Whenever possible, people should be kept honestly informed and updated. The authorities should objectively highlight the risks and issues but promote the counter measures too. They should also explain in simple terms why certain restrictions may be necessary but stress their temporary nature. It is also recommended to inform the community about the additional event related spending that the major event will be feeding in to the local economy and how the community will benefit in the longer term from the infrastructure enhancements the security planners intend to make to support the policing operation. A successful event can very positively promote an area and for a long time after attract the tourism, trade and business that will enhance the economy and deliver opportunities to keep developing safer communities and designing out crime and disorder.

- **Training, Procurement and Practice**: There are also tangible legacy benefits that come about through training staff, procuring equipment and developing practice for security solutions and situations, both actual and contingency, that are either new or have not been experienced or addressed for some time as a result of which the prevailing response is incomplete or redundant. Legacy in this domain would include:
  - Renovating outdated accommodation to have a longer term future instead of incurring costs renting temporary facilities with no sustainable advantages.
  - Moving away from the concept of multi skilling individual members of staff to produce a more widespread and resilient skill base to withstand, within a longer term strategy, major event demands, abstractions for training, gaps arising through retirement and resignation, and availability of personnel on a 24/7 basis.
  - Enhancing LAN, WAN, computer and telephony infrastructures in such a way that as well as satisfying major event requirements, longer term benefits for day to day operational demands will be realised in terms of speed, capacity, compatibility and functionality.

  - The avoidance of products and systems with contractual elements, expensive support packages and costly licences that preclude opportunities to enhance or adapt the systems in the future to meet developing or emerging needs.
  - Realising best value by out-sourcing aspects of planning that can be done equally well, if not better, by less expensive and perhaps better qualified practitioners thereby releasing security personnel to focus on security governance matters.
  - The testing of personnel prior to their appointment as security planners on their ability to sit comfortably and deliver security governance benefits in a legacy culture and climate.
  - Considering locating planning activities or carrying out training exercises in higher crime areas where the increased presence of law enforcement officials will inevitably reduce crime and enhance public safety.
  - Offering the experience and opportunity to be involved in the planning and delivery of major event security to a much wider audience by inviting participation from national and international counterparts – preferably productively but at least as observers.
  - Taking advantage of the major event community based education programmes, to introduce the longer term, less event-orientated and more general concepts of crime prevention, designing out crime, community involvement and public safety.
  - Avoidance of the term “bigger”, with more focus on the word “better”.

- **Environmental Matters**: the impact on the environment of a security operation cannot, and should not, be ignored. There are many ideas that can help to ensure the security plan is ecologically and environmentally sound:
  - If time and location permits, plant suitable “defensive” shrubs, bushes and trees to create cordons and ‘lines in the sand’ as opposed to the much more expensive temporary erections that could be classed as very environmentally unfriendly.
  - For aerial surveillance, utilise tethered blimps instead of helicopters and fixed wing aircraft.
  - Distribute staff refreshments in recyclable bottles and containers.
  - Manage rubbish, waste and water effectively.
  - Engage professional assistance to remove waste.

- Consider acquiring for use vehicles built or adapted to use alternative fuels.
- Avoid building temporary structures on land of significant scientific interest and wherever possible, try and avoid driving off-road in countryside and conservation areas.
- Know and apply national and international legislation designed to protect the environment below the ground, on the surface and in the air.
- Avoid activities that may release or spill contaminants such as petrol and oil, contaminated water or any other liquid that may be hazardous.
- Careful monitor the health of staff and attendees to prevent the spread of disease.

3.2 Capacity

Capacity is the constituent that security planners have at their disposal in terms of human, physical and technological resources.

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 distract them from their event related tasks. In this respect, there should be no misunderstanding 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.

Human resources

The scale of major event planning almost always considerably exceeds that initially envisaged. The complexity around establishing how many human, physical and technological resources are required to populate the security plans is seldom recognised. Neither is it often understood at the outset that a major event may well almost exhaust national resource reserves in some aspects of operational activity, physical security and transport requirements.

It is therefore important that planners determine and select the correct number of trained, qualified and properly equipped staff across the range of security skill disciplines.

A workable shift rotation pattern, toilets for staff, shelters for horses and dogs, the prevention of food poisoning, the charging of thousands of radio and mobile telephone batteries, the secure storage of firearms and even the availability of insect repellent are just a few of the numerous staff related challenges that will arise and have to be addressed by planners.

The need to effectively resource the major event security plan also has to be matched against the reality that as near normal as possible policing arrangements will still have to be applied in areas away from that subject to the special arrangements for the major event. This factor alone has a significant impact on the availability of staff and equipment and major event planners need to work closely with operational colleagues planning day-to-day activities to achieve the best possible use of resources.

The main aspect of planning **Human Resources and Logistical Support** is to determine whether the initial concept of a plan is achievable in terms of the number of trained, qualified and properly equipped staff, across the range of security skill disciplines, required to populate it. That is to say, there is no point in continuing to progress a conceptual plan if the resources required to implement it are either not available, lack the skills or equipment required, or if there is insufficient financial support to pay for it.

This can be done through a **Strategic Resource Audit** process that involves looking at each venue, or part of a venue, or other identifiable area that will come within the major event operation, in isolation. Each isolated area is then sub-divided into zones and each zone is then examined to determine the number of specialist and non-specialist staff required. This time consuming but very important process needs to be conducted by very objective, pragmatic and knowledgeable staff with a wide range of policing skills and security experience. The totals for each area are added and matched against the number of staff that research has forecast as available for the operation. Care should be applied to ensure that any such forecast is accurate and that multi-skilled officers for instance have not been “double counted”. The outcome will determine whether or not the “concept’ plan is feasible. If it is, planning can continue along the lines envisaged. If not, a revised or even new ‘concept’ will have to be designed.

The Strategic Resource Audit must however take into account that security arrangements will have to be robust 24 hours a day for several days. Security arrangements may have to be in place some days before the official start of the event and may have to remain at the end thereof for the deconstruction phase of the operation. Legislation may prescribe that officers may only work certain periods before being given specific periods of rest. They may have to be accommodated some distance away from their place of duty and accordingly time for travelling and getting access to the site, equipping, briefing and deployment on site will have to be built in to shift timetabling.

Other considerations may have to include matters such as cancelling all training, days off and even in some cases, annual leave. The knock on effect of such decisions is significant in terms of longer term operational effectiveness and decisions such as these may not be popular or well received by staff. A good working relationship with staff unions and associations throughout the planning and event periods can be particularly beneficial in terms of negotiating the best possible staffing arrangements.

The complexities around planning staffing and logistical matters are significant and the importance of taking the time to select intelligent, committed, sensible and professional staff to fulfil these functions has to be promoted in the strongest possible terms.

Logistics

Having determined, as accurately as can be expected, the number of police and security staff required to populate the plan, the locations they are going to be deployed and in what roles, work can begin in earnest to organise the requisite logistics to support the deployed personnel.

This can be done as a second phase of the Strategic Resource Audit with the previously identified zones or other areas of activity being revisited but this time with the personnel and the roles they are to fulfil marked thereupon.

Logistics planners then ascertain what will be required - firstly what is needed when the personnel are deployed out in the field in terms of additional personal equipment, vehicles, food and shelter for instance. Secondly they have to determine food and lodging for the personnel when not deployed, how they are going to be delivered from that accommodation to the site and what additional, possibly temporary, accommodation is required to support the agreed logistics plan.

As before, having gone through this exercise, the results are totalled and further research is conducted to confirm supply can meet demand. Again, if demand exceeds supply, it may be the case that the staffing and / or logistics plan needs to be reviewed in one area or more to get the balance right.

It should once again be re-iterated that if done properly, this is a particularly complex and time consuming task. Transporting, for example, 10,000 personnel a day from accommodation to site and thereafter from site to deployment point is not an insignificant task and the arrangements required to secure such a large number of vehicles for the purpose are considerable – provided that around 200 coaches and 600 drivers per 24 hour period can actually be procured at a reasonable cost. The same issues tend to apply across the logistics planning template and there is a distinct likelihood that in several logistics planning areas, demand will actually exceed the national supply stock, being quite apart from the normal daily requirements, aspects of the event separate from security, will be placing similar demands on the available supply stock. Major events for instance may attract several thousand journalists, who will want to be transported by coach. Event organisers will also be seeking to procure coaches to transport several thousand delegates and/or athletes – and of course, as demand for limited supply increases, so too does cost.

Amalgamation

There are several tools and practices that may help planners to match what is expected, planned and practiced.

1) Plans: practices to help integration

The first tool is designed to support integration. "Integrative days" involve planning representatives jointly reflecting on known interdependencies with the aim of confirming that the matter has been effectively addressed in the planning process.

Based upon an assumption that "clear things are often in fact muddled", some key questions can be asked in these sessions to make sure nothing is assumed or taken for granted:

- Who does what, when and how?
- Is everybody working within the same planning schedule?
- When and where do plans come together?
- Where are the gaps?
- Who will fill the gaps?
- Is there any duplication?

Integration days are effective when open questions are asked and participants are required to comprehensively respond. Wall charts and time lines can be used to assist the process. Sessions should be interactive and all key organisation involved.

Known phrases of security planners reflect the need for interaction: "The plan is nothing, planning is everything"; "when the plan is ready, it is time for planning", "If you fail to plan, you plan to fail" or "it's the planning that gets you there, not the plan".

2) People: practices to promote compliance

People involved in major event security can only be expected to accommodate a limited number of new procedures. More often then not, the behaviour of individuals will not change much – they will largely behave as they are used to behaving.

Following this general rule, planners should be very careful to not introduce too many new or complicated procedures. Planners should keep a keen eye on those procedures that are regularly used by personnel involved and resist the temptation to do something too innovative.

A simple tool to support the introduction of new procedures is to graphically highlight those that deviate from recognised standard operating procedures. Another supporting tool is to have pocket books or something similar that contain “must know” information, up-to date procedures and other essential data.

Manuals can also be produced and circulated. For example, at the 2000 Salt Lake Winter Olympic Games a Public Safety Standard Operating Procedures manual was published. This manual contained important phone numbers, checklists how to deal with various emergency situations. It also contained site maps, flowcharts, timetables, distance charts, bomb threat forms and reporting formats.

3) Sites: practices to test venue security

The best-laid plans may not survive the first event day if real-time checks have not taken place prior to the event starting. Safety and security procedures also need to be considered in this regard. There are different ways to test plans through exercises, education and training.

Test events allow authorities to evaluate procedures on a wide range of general safety and security issues. They may also generate an opportunity to validate the number of personnel and the type of equipment identified through the earlier mentioned Strategic Resource Audit. Also they reveal mishaps, forgotten items and potential problems that do not always come up on paper.

3.3 Constraints

Human, physical and technological resources are subject to different constraints that restrict and regulate their application. Therefore it is important that security planners and managers research and understand these constraints prior to committing resources to any aspect of planning or operational activity during the major event. Constraints can include financial, time-related, legal as well as image and political factors.

Financial factors

Costs and the **sourcing of funds** can lead to major challenges. Budgets of major events may differ depending on characteristics of the events such as the size, location and purpose, the duration, and different safety and security requirements. Costs have to be realistically limited to fall within the budget available. In any case, the cost to secure a major event is likely to be very large, running into tens and even hundreds of millions of dollars. By way of example of where the major costs will lie, the table below highlights in very broad terms the cost of providing security for G8 Summit 2005. As tends to be the case in policing and security matters, a very large percentage of the costs were consumed paying staff wages and allowances.

G8 Summit 2005 COSTS	
Planning Costs	12.251
Staff Costs	44.660
IT and Office Equipment	1.151
Staff Accommodation	3.008
Transport/Mobilisation Provision	3.369
Catering for the Event	1.219
Air Support	0.437
Insurance	0.499
Gleneagles Perimeter Security	0.882
Temporary Structures	0.755
Private Security	0.477
Staging Posts	0.168
Equipment	1.197
Airwave	0.367
Airport physical security	0.411
Miscellaneous	1.125
TOTAL	**£71.976m**

Ineffective budgeting can obviously negatively affect the planning process but sound financial management practice may involve the use of several approaches to be able to define cost-benefits more precisely. These involve modelling security budgets, using benchmarks with past major events, risk analysis of security costs and methods for cost-benefit analysis.

The financial management of such large budgets is clearly a complex matter and individuals with responsibility therefore obviously have to be properly qualified. Questions that may be asked from both internal and external sources on the subject of budgetary control include the following and accordingly, planning members of staff should have sufficient understanding to respond to:

- What is the security budget?
- Which budget pays for what?
- What are the likely staff costs?
- What are the other costs?
- Of the total budget, what percentage is going on safety and security?
- How do the costs benchmark against similar events in the past?
- What are the security costs per ticket sold – and how does this compare?

It is possible to identify some other good practices with regard to safety and security costs. First, key drivers of safety and security costs are the numbers of police, medical staff and other emergency personnel that are on duty at any time during the event. Thus budgets can be predicted to a great extent by calculating the expected number of personnel needed times their hourly cost. These expenditures may differ between host countries due to national differences in paid rates. The identification of a few key drivers such as personnel costs and equipment may help to simplify the budgetary process and control.

Moreover, control of safety and security budgets depends on several critical success factors. Lack of sufficient control of these factors may introduce risks of budget overruns. These risks should be explicitly recognised for instance by performing sensitivity analysis of budgets. Examples of such analysis can be found in studies of economic feasibility of major sporting events.[2]

[2] Kurscheidt, M. Strategic Management and Cost-Benefit Analysis of Major Sporting Events, University of Paderborn, 2000.

Time factors

One of the keys to a successful event is to start planning early, maybe even several years before the event is scheduled to take place. Although this position is widely recognised as a critical success factor, it often proves difficult to initiate a meaningful planning operation when the event seems such a long way off. Authorities, for instance, perhaps find it difficult to dedicate personnel to planning because of other demands on their time.

If it is agreed to host a security conference, to which law enforcement and security personnel officials from participating countries will be invited to attend at a relatively early date in the planning process calendar, the need to have plans and measures prepared at least to a concept stage and ready to present may assist to focus attention in a meaningful way.

The time available for planning will quickly disappear and 'interested' observers will quickly highlight shortcomings. It is therefore very important to try to maintain confidentiality, keep things in perspective and 'get it right first time'. The more people involved in the early stages of planning, the harder it is to achieve this.

The table below shows the start time for planning in respect to the event times of different Olympic Games:

Olympics	Planning Start	Games Time
Barcelona	01.01.1988	10.07.1992
Lillehammer	01.02.1989	12.02.1994
Atlanta	10.09.1991	19.07.1996
Salt Lake City	01.03.1998	08.02.2002
Athens	01.08.2000	13.08.2004
Torino	11.10.2001	10.02.2006

Legal factors

All security activities have to be conducted within the bounds of the law. Besides the legal parameters set within domestic law, the conduct of all security agency personnel involved should meet international standards outlined in provisions such as the United Nations Code of Conduct for Law Enforcement Officials and the United Nations Basic Principles on the Use of Force and Firearms by Law Enforcement Officials.

Moreover, as major events may involve extraordinary decisions not supported by existing legislation, additional legislation may be required. We may distinguish between the following types of legislation.

Firstly, temporary or permanent special legislation may be needed to support the organisation of the major event. For instance, Utah introduced legislation to bring in a new agency with a specific role for the Salt Lake Games in 2002. Among other things, this legislation defined the mandate of public authorities and specified the division of tasks and responsibilities between public and private partners. At Lillehammer in 1994, temporary provisions were instituted to support the security measures and restrict access to the city in certain circumstances.

Secondly, special judicial arrangements in courts may be necessary in terms of matters such as:

- the level of penalties for different types of offences committed during the event;
- the option to use summary proceedings to speed up the legal process;
- the organisation and operation of the courts, including improved capacity, organisation and procedures for additional sittings and powers of detention;
- creating injunctions to prohibit access to event-related venues;
- the provisions for the expulsion of foreign nationals;
- temporary border controls (art 2.2 Schengen Treaty);
- the use of surveillance equipment in public places.

Thirdly, sites and equipment are usually licensed by competent authorities prior to the event. The aim of licensing is to ensure compliance with safety and security standards. Licensing and safety certification is often done by different agencies acting as competent authorities.

The necessary scope and detail of the legislation depends to a large extent on the legal provisions that already exist in the host country. It needs to be understood, however, that the introduction of new provisions may be controversial as they may be seen to infringe on the constitutional rights of individuals.

Image and political factors

Major events may bring disruption to normal business and community life in general. Major event venues, celebration sites, Olympic villages, etc. normally have a very high level of security involving fencing systems, buffer zones, and a variety of search and detection equipment and procedures that perhaps appear to restrict normal life. Scrutiny and criticism from internal and external bodies, and the pressure to satisfy the widest imaginable range of stakeholders may be significant.

Moreover, from a national perspective, given the significance of hosting a major event, there will inevitably be a great deal of political interest in all aspects of the operation at every governmental level.

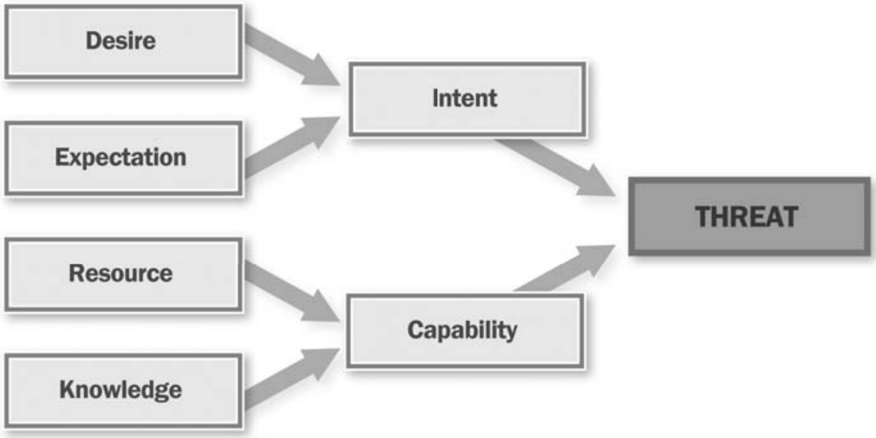
It is therefore important that security is planned and provided by finding the right balance between protecting the event and preserving as much as possible a peaceful environment in the event area. Image and political factors must therefore be taken into account when planning.

3.4 Intelligence

Risks can seldom be totally eliminated but they can be significantly minimised 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.

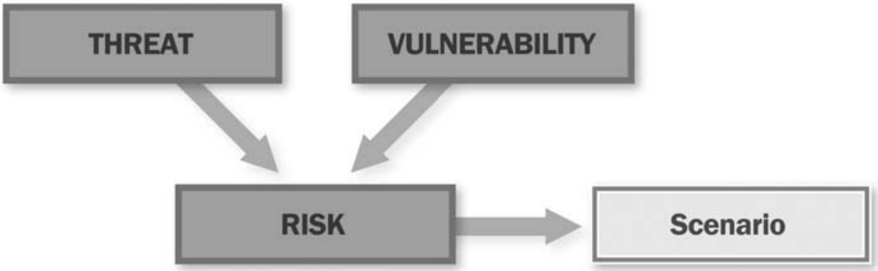
Ideally intelligence should provide:

- 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. As shown in the figure below, 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.
- 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. Vulnerability assessments need to take into account the plans of all parties involved. The vulnerability



assessment of sites may be easier than that for subjects that may be vulnerable to attack. Sites are fixed, the numbers of sites are limited so their design and layout can be reviewed alongside security plans. For vulnerable groups or individuals the situation is different as it involves assessing many different people or groups with different needs. Moreover, threats can change over time and the level of protection and the effectiveness of such measures will differ from group to group.

- 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.[3]



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

Intelligence activities play a fundamental role both during the planning process and during the major event and can:

- Help planners, commanders and key partners to best decide where resources should be allocated.
- Provide strategic and tactical commanders with regular threat and vulnerability assessments in order to identify possible risks related to protection of groups such as the public, dignitaries and athletes, as well as the protection of venues and non-venue sites, critical infrastructure, transport and specific ceremonies such as opening and closing ceremonies or torch relays during Olympic Games.
- Provide high quality, live-time and assessed intelligence reports to guide the strategic and tactical commanders in timely deploying police resources
- Provide operational commanders with live-time quality intelligence to enable them to pro-actively deal with situations before they arise.

Chapter 4

The Deliverables

The component Deliverables can be defined as the complementary set of security plans that the System designs and delivers to:

- 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**),
- be prepared in security related contingency planning terms (**if**).

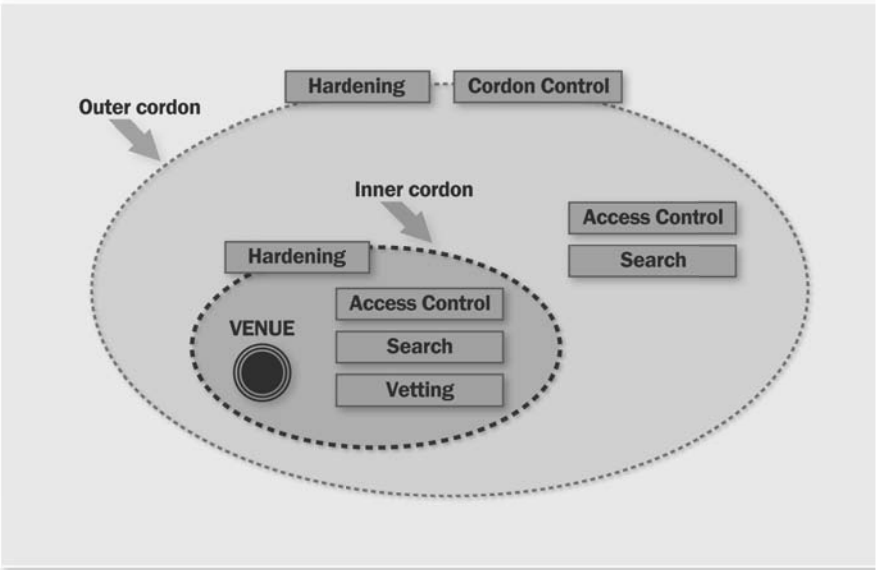
The table below shows how in each of the three main categories of complementary plans (‘inside’, ‘outside’ and ‘if’), which people need to be protected, where they have to be protected and how they can be protected. Within the normal course of designing a security plan, it is imperative to recognise 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 broad view should consider the nature of any potential threat so that it can be identified, anticipated and stopped before striking the potential target(s).

Deliverable			
	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

4.1 Plans inside the designated secure area

The purpose of these plans is to prepare a package of strategic measures that should intercept problems and threats before they reach participants, spectators as well as security and non-security staff inside the secure area. Usually the security area around the venues is composed of different security layers or “island sites”. **Inner cordons** are used to control access to the immediate venue event. Access to the area controlled by an inner cordon should be restricted to a limited number of people. **Buffer zones** and **outer cordons** are appropriately created to prevent an attack on the area within the inner event cordon.

The nature of the event and risk/vulnerability/threat factors means different strategies will be employed as required to protect life and property inside the designed secure area. As shown in the figure below, IPO has taken into consideration and discussed a number of such strategies to be further elaborated on below.



- **Securing and hardening the designated secure area**: when appropriate, the security areas can be protected by **physical and technical means** using for instance 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.

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?

- **Search and surveillance**: 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.

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”?

- **Cordon control**: the aim is to apply adequate policing strategies to ensure a secure and uninterrupted major event, facilitate lawful protest and, when necessary, organise proactive engagement with individuals or groups challenging the security measures. To prevent and effectively respond to disorder and violent demonstrations, it is important to understand crowd behaviour. Crowd management includes options such as pre-meetings with group organisers, community education, the deployment of sufficient numbers of law enforcement staff to anticipate events, the separation of opposing factions, the maintenance of contact with the crowd and the establishment of rules of conduct. Protester tactics are dynamic and require a flexible response. Security agencies 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 horses and dogs, and the use of less lethal options such as chemical agents, water cannons, taser and baton rounds.

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?

- **Vetting validation and accreditation**: the aim is to prevent infiltration of the venue event by persons who are not entitled to be there. 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, recognising the identity of ticket holders and preventing potential perpetrators from buying tickets.

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?

- **Access control**: the aim is to control the different venue access and egress points for different categories of persons such as delegates, media, participants, athletes etc to prevent unauthorised entry and, at screening stations, identify threats to the event through the use of metal detectors, bag searches, etc. 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?

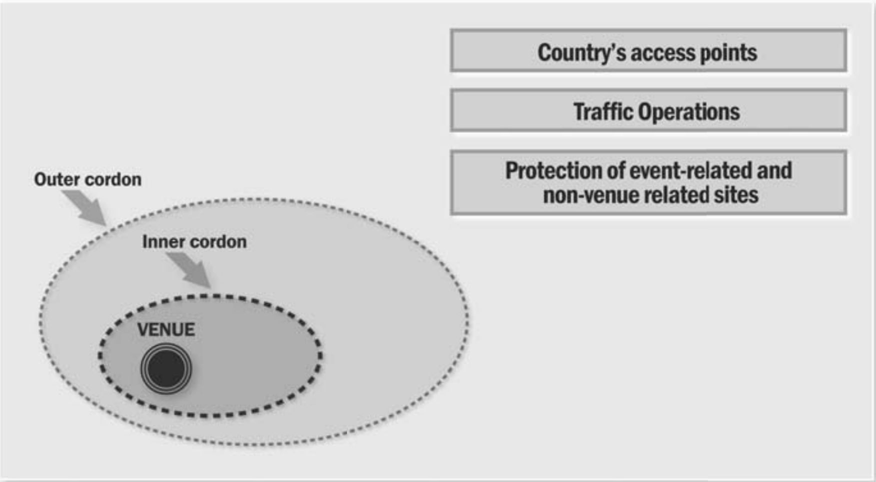
- **Dignitary protection**: these are precautionary, preparatory and proactive measures that ensure the security of individuals deemed to be at risk. The main aim is to protect specific groups or individuals, for instance Dignitaries, VIPs and Athletes.

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?

4.2 Plans outside the designated secure area

The aim of these plans is to prepare a package of strategic measures that are designed to intercept problems before they reach the secure venue area and protect the wider community at large. As shown in the figure below, IPO has taken into consideration and discussed a number of tools further outlined below.



The main tools that the security planners have at their disposal include:

- **Control of country access points (land, sea and air)**: the aim is 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.

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?

- **Traffic operations**: this relates to all measures needed to:
  - Maintain and secure access routes to and from venues and other designated places for delegates, media, police resources and others, which includes the management of road closures and other tactics involving for instance, the saturation and securing of critical and alternative routes.
  - Maintain 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.

- Design a public transportation system that is capable of handling expected volumes of people at given times and places in a safe and secure way.
- Prepare 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.

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?

- **Protection of non-event and event-related sites**: security planners should design tactical options to protect participants, staff and the community outside the designated secure event area. In particular:
  - **Event-related sites**: hotels where participants and staff stay, sponsor villages, media centres or sites designed for leisure management such as fan parks.
  - **Non-event sites**: including:
    - **Critical infrastructures**: infrastructures that the country hosting the major event considers as “critical” for purposes of national security. Critical infrastructures may include nuclear and chemical industry and installations, the utilities, communications and key transportation links.
    - **Other soft targets**: places within the civilian population of a country or its infrastructure that are particularly vulnerable to penetration and attack by terrorists. It could include shopping centres, tourist locations, historical monuments etc.

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 health, governance, the economy and national 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 through which public authorities, private sectors and private citizens can cooperate through a multi agency approach. Security planners should be able to explain to the community that any disruption of event-related and non-event related sites could adversely affect the State.
- **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.

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?

4.3 Contingency Plans

The strategic aim of this deliverable is to both counter emerging threats and respond when unexpected situations arise. Areas where contingency plans are required include possible fires, explosions, terrorism, CBRN attacks, suicide attacks, structural failure, crowd disorder, power failure, safety equipment failure, off-site hazard etc. It is important to appreciate that also a minor incident could scale to a major one if it is not properly managed. Contingency plans should deliver emergency responses wherever they are required. There are some main basic principles which may be incorporated into contingency planning:

- **Combined and coordinated management**: contingency plans should be based on a multi-agency approach that includes event organisers, police, health authorities, fire authorities, local authorities, private sector organisations (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. Contingency plans should consider and where possible integrate existing working procedures and existing local authorities emergency planning.
- **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. There is no one model respond to every emergency. Responses need to be flexible and vary according to the nature and effects of the crisis. However there are some common objectives that characterise all emergency responses. These objectives should include:
  - Saving and protecting life and property.
  - Treating, rescuing, and transporting casualties.
  - Containing the emergency and the casualties (including stopping the event, evacuating the audience from the venue).
  - Managing evacuation.

- Safeguarding the environment.
- Maintaining critical services.
- Providing the media with information.
- Restoring normality as soon as possible.
- Facilitating investigations and inquiries, ensuring that the scene and any other evidence is preserved,.

- **Training and exercising**: it is important to test the effectiveness of plans and the competence of all individuals or groups involved. A possible tactic would be to hold frequent meetings with relevant personnel to exchange information, build team spirit and encourage networking. It is also important to schedule training exercises, use progressive training (from classroom sessions to tabletop exercises) and divide training programmes into subcategories such as speciality training, field exercises, product/equipment training etc.

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)?

Chapter 5

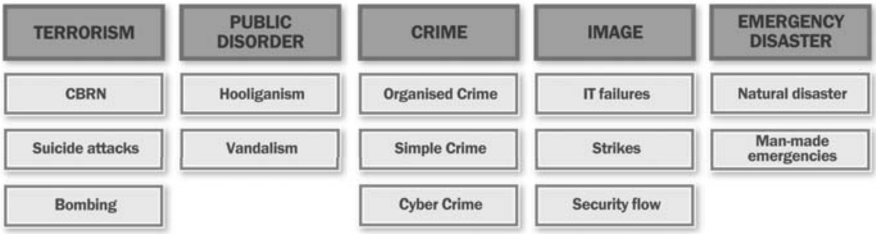
The Risks

The component Risk indicates the presence of adverse events that may expose community, critical infrastructures and other soft targets to the possibility of being injured or attacked during a major event. Risks may include:

- **Terrorism**: terrorist attacks at major events in the past have altered the design of major event security today. The Black September attacks on the 1972 Munich Summer Games were the watershed that permanently changed the conceptualisation of risk and management of security at major events. The bombing during the 1996 Atlanta Summer Games also demonstrated the fragile nature of security at large scale public gatherings with multiple avenues of access, thousands of spectators and participants, and of course, the wider community at large. The fact that the bomb exploded at the Centennial Park illustrated that the vulnerabilities were not simply related to the event venue itself, but also to event-related or non-event-related sites. Recently, security planners have been concerned by new forms of transnational terrorist networks that, as demonstrated by the recent international terrorist attacks, are growing more international in their scope and less predictable in their use of violence. Current concerns for acts of terrorism include the use of CBRN weapons (radiological dispersal devices, nuclear blasts, biological and chemical threats) and suicide attacks. In this arena, security planners have strengthened contingency plans to preserve and protect life, minimise the impact of the incident, support the decontamination process, inform the public and maintain public confidence. International events and the foreign policy of the hosting countries should be also taken into consideration as matters that may influence terrorist behaviour. For example, the presence of national military in foreign missions or the participation in the major event of countries that are directly involved in the international fight against terrorism have recently led security planners to reinforce security measures to prevent terrorist attacks from Al Qaida or similar groups.

- **Public disorder**: this category involves different types of disturbances, including sports-related violence (hooliganism), fights, molestation or vandalism, unlawful assemblies and demonstrations, disruption to the transport infrastructures, wilful damage to property, and the occupation of buildings. In the past, the most serious spontaneous public disorder was associated with hooliganism at large sporting events in general and football matches in particular, as demonstrated by the dramatic case of the UEFA Champions League in 1985 in the Heysel Stadium in Brussels (Belgium) when the behaviour of hooliganism caused the collapse of a wall and the death of 39 people. Today security planners dedicate a great deal of attention to the security of events that attract local or foreign protesters, such as anti-globalisation protesters or other groups that intend to use a major event as a vehicle for publicising their causes. In particular, political major events such as G8 summits can attract peaceful but also violent protestors. In this arena, the central issue, as well as supporting human rights, is handling crowds both in terms of "proactive" crowd management and "reactive" crowd control. Security planners' priorities are to facilitate peaceful protests, minimise a whole range of risks and, where necessary, intervene to avoid disruption. It is important to underline that excessive or poor crowd management and crowd control can significantly jeopardise community safety.
- **Crime**: this category refers to both organised crime and common crime. Recent major events demonstrated that the most common crimes are ticket forgery, pick pocketing in crowded places (Metro, subways stations, public squares, shopping centres etc.), bag thefts, etc.
- **Image embarrassment**: this includes any sort of conduct by an individual or group designed to not present a threat in terms of breaching security but rather in a number of different ways to seek to discredit or embarrass the event or any one or more of the bodies involved in its organisation. Such conduct can take a number of different forms including "sensational" media disclosure of flaws in security, strikes and "comic terrorists" presenting themselves as "Batman" or "Spiderman". Media interest during such occurrences is likely to be significant and the preparation of contingency plans and suitable responses in this regard should be considered.
- **Accidents, Emergencies and Disasters**: this category is self-explanatory and includes fires, traffic accidents, earthquakes, hurricanes, nuclear plant accidents and dam failures. Infectious disease, food poisoning or hazardous material incidents before or during a major event may also be included in this category.

All the forgoing risk categories can branch into several different types of incidents or hazard events as shown in the table below. Each category can be refined or sub-divided depending on the level of analysis is chosen. Moreover, risks can be interconnected. The consequences of a natural, human or technological accident could be magnified by the presence of large crowds and international media. As risks can be interdependent, ripple effects can occur and, if not properly managed, seemingly small incidents can spiral out of hand.



TERRORISM	PUBLIC DISORDER	CRIME	IMAGE	EMERGENCY DISASTER
CBRN	Hooliganism	Organised Crime	IT failures	Natural disaster
Suicide attacks	Vandalism	Simple Crime	Strikes	Man-made emergencies
Bombing		Cyber Crime	Security flow	

Chapter 6

IPO Assistance

This IPO Security Planning Model has been designed to try to simplify the complex task of planning security for major events and it hopefully provides a sensible and pragmatic model that identifies the main components of the planning process and the principal issues around each such component.

It attempts to demonstrate that security planners face significant challenges in terms of developing comprehensive, resource intensive and expensive arrangements to protect major event venues, people attending them and the local residents. Although major events often uphold principles of freedom and justice, there are many potential threats that undermine their safety and security ranging from hooliganism to terrorist attacks. In addition, planners have to cope with limited financial support, significant political pressure, massive media interest, community concern and possibly little experience.

For this reason, the IPO Security Planning Model is designed to fill a number of identified gaps and IPO now offers a number of services based thereon, across the widest possible range of security topics from, for instance, command & control to venue and non-venue security, project management to personal protection and logistics to counter terrorism contingency planning. IPO mentoring and quality-assurance services are delivered around the priorities identified by the Member State hosting the major event and thereafter further refined during an IPO needs-assessment mission.

For obvious reasons, the remit of IPO does not extend to involvement in actual operational activity or the provision of assessed intelligence, but UNICRI can promote knowledge exchange and offer the best practice on mechanisms for gathering and processing information. With the support of the relevant National Authority, Organising Committees can also seek their support of IPO mentoring and quality-assurance services.

Information on how to obtain IPO assistance, and details on the collection, analysis and dissemination of best practice on major events security can be found on the IPO website (www.unicri-ipo.org).