OAS More rights for more people

unicri United Nations Interregional Crime and Justice Research Institute

Security Planning on a Large Scale:

A Practical Manual

OAS Cataloging-in-Publication Data

Security Planning on a Large Scale: A Practical Manual / [Prepared by the Inter-American Committee against Terrorism of the General Secretariat of the Organization of American States (OAS/CICTE) and the United Nations Interregional Crime and Justice Research Institute (UNICRI)].

v. ; cm. (OAS. Official records; OEA/Ser.L/X.6.2)

ISBN 978-0-8270-7502-3

1. Security, International--Handbooks, manuals, etc. 2. Public safety--Handbooks, manuals, etc. 3. Infrastructure—Security measures—Handbooks, manuals, etc. 4. Computer security. I. Title. II. Organization of American States. Secretariat for Multidimensional Security. Interamerican Committee Against Terrorism. III. United Nations Interregional Crime and Justice Research Institute. IV. Series.

OEA/Ser.L/X.6.2
OEA/Ser.L/X.6.2

With the financial support of the Government of Canada Canada

Content

Preface

Public security is always a top priority for governments, and nowhere is that clearer than at a public event that draws international attention or large crowds. This manual aims to provide practical guidance to enable national policy makers, government bodies, law enforcement agencies, and other stakeholders to identify, coordinate, and organize the many and varied aspects that go into any multifaceted security plan. It is based on the security planning process for major events such as international sporting competitions or presidential summits—which typically involve months or even years of preparation and thousands of players—but it can be adapted to other security situations as well.

Security is an increasingly complex task in a world of ever-evolving risks. The United Nations and other international organizations have adopted many international programs and instruments to strengthen their ability to work together on this front. These include, to name just a few of the most relevant:

- **UN Global Counter-Terrorism Strategy (2006), a shared plan of action to fight terrorism;**
- **Resolution 2006/28 of the UN Economic and Social Council, "International Permanent Observatory on Security Measures during Major Events;**
- **UN Security Council Resolutions 2341 and 2396 (both from 2017), the former on protecting critical infrastructure and the latter on strengthening information sharing and judicial cooperation; and**
- **2015 Madrid Guiding Principles, intended to stem the flow of foreign terrorist fighters, as well as an addendum to those principles (2018), which covers issues related to the protection of critical infrastructure, vulnerable or soft targets, and tourism sites.**

Within this framework, the Organization of American States (OAS), through its Inter-American Committee against Terrorism (OAS/CICTE), and the United Nations Interregional Crime and Justice Research Institute (UNICRI) have partnered for many years to develop a body of best practices related to security at major events and tourism destinations. Through one of their earliest projects, they provided technical assistance to 10 Caribbean countries in advance of the 2007 Cricket World Cup held in the West Indies. The OAS/CICTE and UNICRI have continued to work together throughout the Americas to promote integrated planning, public-private partnerships, community engagement, and regional cooperation in this area. In 2020, they launched their latest collaboration, called Improving Crime Prevention Policies and International Cooperation for the Protection of Crowded Spaces and other Vulnerable Targets—the Protection of Crowded Spaces Program for short.

This manual was produced as part of that program. It builds on the UNICRI Security Planning Model first published in 2007—in the context of the UNICRI International Permanent Observatory on Security Measures during Major Events—and consolidates the considerable know-how acquired by UNICRI and the OAS/CICTE over the years.

The central aim of this manual is to provide an organizing framework and a tested methodology that can be used to analyze the entire planning cycle of any large security undertaking and efficiently design and implement plans to protect crowded spaces and vulnerable targets. It is based on a version of a process mapping tool often used in business, called a **SIPOC** diagram; the acronym stands for:

Sources
Inputs
Process
Outputs
Customers

The SIPOC approach offers a high-level organizing framework and a common reference point for everyone involved in the security plan. It also makes it easier to identify and isolate specific tasks and roles, thanks to detailed steps and guidelines included in each of the areas.

This updated version of the UNICRI Security Planning Model benefited from the valuable inputs and contributions of Brendan Heffernan and Brian London, now-retired members of the Royal Canadian Mounted Police (RCMP), who have extensive experience in security planning for major events hosted by Canada. Duccio Mazarese, Alice Roberti, and Danielle Hull of UNICRI worked on the document and provided guidance through the drafting phase, while Paola Fernández, Andrea Rodríguez, and Eduardo Granizo at the OAS/CICTE provided overall coordination. Finally, the OAS/CICTE and UNICRI express their gratitude and appreciation to the government of Canada, whose contributions have made their work in security planning possible for more than 15 years.

Introduction

When large numbers of people congregate in one place—whether athletes, spectators, tourists, diplomatic delegations, or protesters—security concerns must be top of mind. The more visible the event or the more crowded the location, the greater the potential vulnerability to malicious acts, whether an assault on a building or a crippling cyberattack. The COVID-19 pandemic has served as a reminder that other types of threats can also pose serious safety risks to the public.

Every event is unique and every place different, but an effective model for security planning can lay a solid foundation on which to build a comprehensive strategy that can then be adapted to specific circumstances. Good planning helps guide the entire decision-making process, making it possible to set clear goals and objectives, quantify needs, align resources, and implement initiatives.

The model laid out in this publication introduces key considerations, identifies strategies, and highlights some of the questions and challenges that go into large-scale security planning. Grounded in international experience and best practices related to major international events, it is intended to assist national authorities and public agencies as well as other organizations and individuals involved in security planning for any type of situations that may involve crowded public spaces or other vulnerable targets.

Of course, security forces and law enforcement agencies in every city and country know their jurisdictions well and have experience in preparing for recurring events. The idea here is to provide decision-makers with a useful framework for events that may require additional levels of security planning because of their size, scope, complexity, or international relevance. Such events often require greater coordination with additional national partners, including with other countries, and often entail significant security risks and intense media scrutiny. For these reasons, planning must be more structured and methodical.

The SIPOC Diagram

The methodology laid out in this manual relies on process mapping, a concept often used in business to visually depict the various phases of a complex process with the aim of designing better systems, addressing challenges, tracking progress, and improving efficiency and results. This particular methodology uses the SIPOC diagram—the acronym stands for **suppliers, inputs, process, outputs,** and **customers**—as a foundation for a comprehensive security plan.

There are any number of planning strategies that can be applied in the security context, and in some cases, decision-makers may opt for a different approach, depending on the financial, geographic, political, or cultural circumstances. One size does not necessary fit all. Regardless of which methodology is used, though, security planning should be based on a solid and efficient reference model.

The SIPOC diagram used in this case provides a straightforward, easy-to-read, and flexible model that can be successfully implemented across different countries and contexts. It prompts planners to analyze all the different security elements and factors to be considered before, during, and after a major event.

Sources

In this context, security planners will depend on three main sources for what they need: the host government, foreign governments, and the private sector or civil society.

Inputs

The raw materials of a security plan are mainly information (including intelligence), resources (human, material, and technological), and obligations (ranging from national legislation to private contracts).

Process

The security planning process, equivalent to the manufacturing process in an industrial setting, takes the inputs and turns them into the final product, which in this case are the plans that will be implemented. The process follows several distinct phases and relies on a highly organized workforce focusing on six different aspects: intelligence, finance, legal, safety and security, logistics, and communications.

Outputs

Three types of products will come out of this process: operations plans, support plans, and communication plans.

Customers

The final beneficiaries include anyone who attends or participates in an event or even watches it on television, as well as local communities and national governments that may see add-on benefits in the form of reputational gains or increased tourist visits. Ultimately, all citizens benefit when the people assigned to protect and serve the public are operating at their best.
For this reason, this manual does not include a chapter dedicated to customers, and it considers their satisfaction as the goal and final result of any successful security plan.

SIPOC DIAGRAM

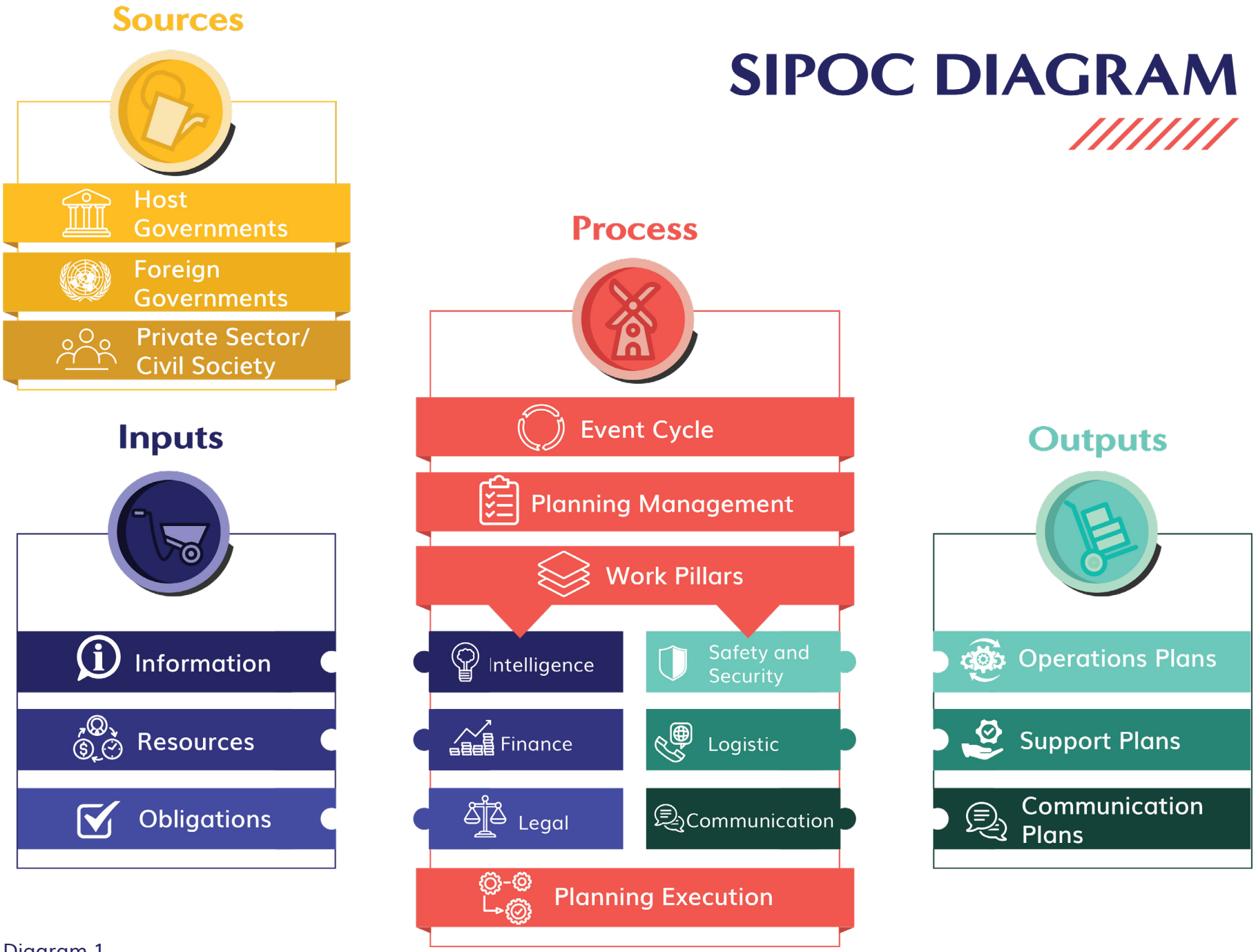


Diagram 1

OUTPUTS

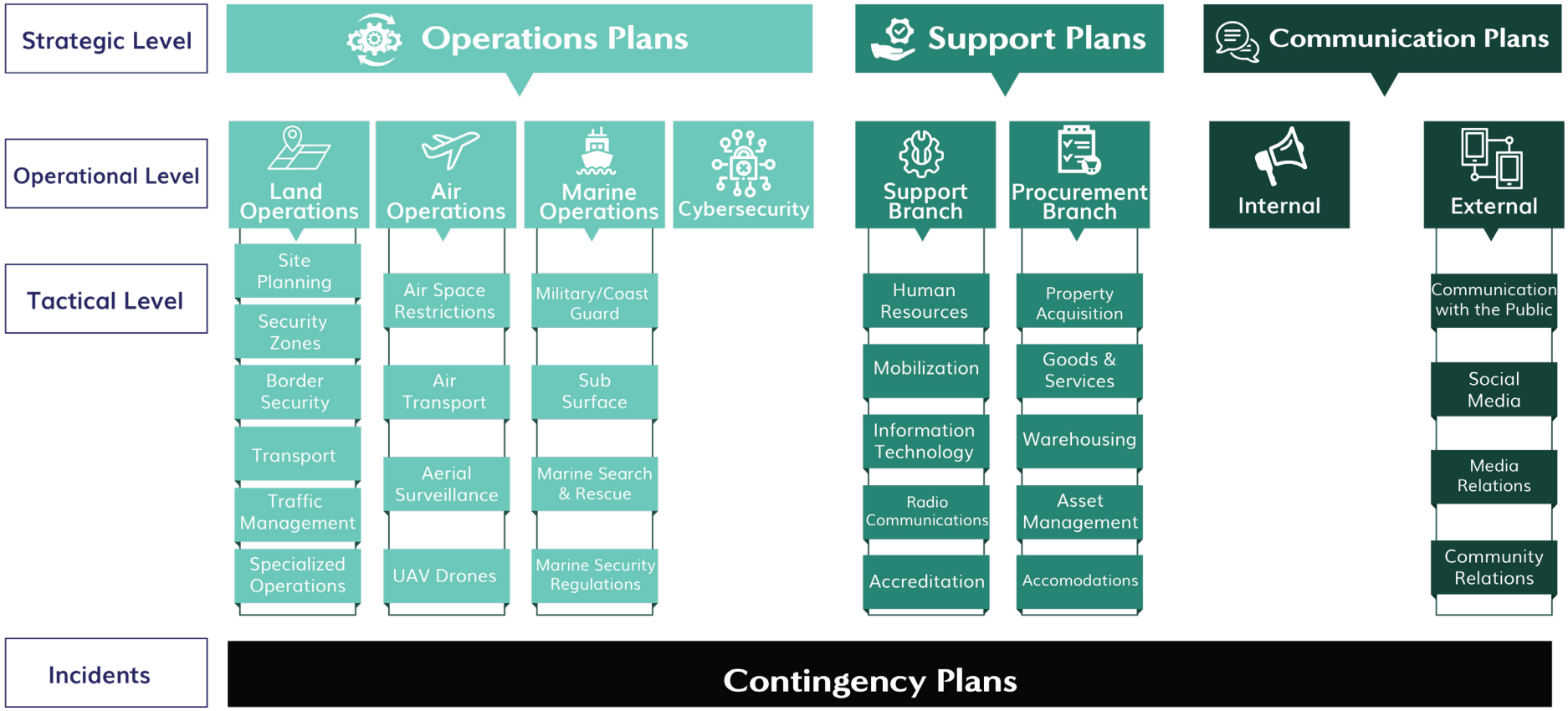


Diagram 2

This manual first provides an overview of guiding principles that should form the foundation of any security undertaking and looks at several cross-cutting considerations likely to come into play. Subsequent chapters examine the nuts and bolts of complex security planning efforts using the SIPOC methodology.

CHAPTER 1: THE PLANNING CONTEXT

Security planning for major events should begin with a broad understanding of context and a good grasp of basic guiding principles that will come into play regardless of the type of event or the host, participants, or location. This chapter touches on a few of the overarching principles for planners to keep in mind[1] and reviews some of the cross-cutting considerations that tend to arise and that should be integrated into security planning from the beginning.

1.1 GUIDING PRINCIPLES

1.1.1 HUMAN RIGHTS

First and foremost, security planning must be aligned with national and international law in the area of human rights, in the spirit of the United Nations Universal Declaration of Human Rights and the American Convention on Human Rights. "Human rights are rights inherent to all human beings, regardless of race, sex, nationality, ethnicity, language, religion, or any other status," as the United Nations puts it.[2] At the core of the broad range of civil, political, cultural, economic, and social rights that are fundamental human rights is the recognition that everyone is entitled to equality, dignity, and respect.

Adherence to human and civil rights must occur at every step of the security process, from the selection of the planning team to the delivery of security services during the event. A commitment to human rights starts at the top, with the security leadership, and must permeate the entire team, including outside contractors. All stakeholders must understand that, whether they are dealing with security staff, members of the local community, or crime suspects, upholding human rights is a non-negotiable obligation.

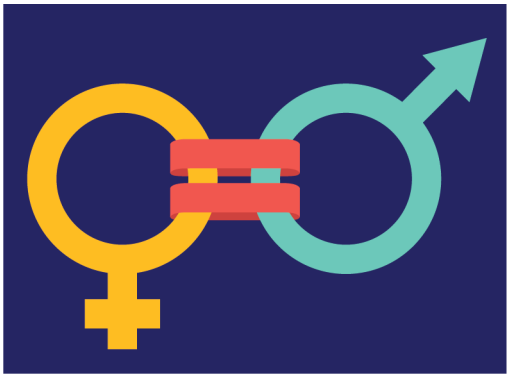
1 For additional considerations on these overarching principles, see: *Guide on the Security of Major Sporting Events – Promoting Sustainable Security and Legacies*, United Nations Office of Counter-Terrorism (UNOCT), United Nations Interregional Crime and Justice Research Institute (UNICRI), United Nations Alliance of Civilizations (UNAOC), International Centre for Sport Security (ICSS), 2021.
2 United Nations website, Global Issues: Human Rights, visited on October 7, 2021.

> These rights, which are safeguarded in international human rights treaties, include the right to life, security of the person, the right not to be tortured, the right not to be arbitrarily arrested, the right to a fair trial, the right not to be discriminated against, the right to freedom of association, the right to freedom of expression, the right to work, the right to health, the right to recreational activities and cultural activities, as well as other rights.[3]

Beyond the moral imperative, the full implementation of human rights in the design and application of security measures is in everyone's best interests. It contributes to transparency, credibility, and good governance; produces security policies that are more reliable and effective; and leads to better relationships with local communities, which can be valuable allies in preventing crime.

1.1.2 GENDER EQUALITY

A commitment to human rights includes respect for gender equality. The security planning leadership must integrate a gender perspective into every stage of planning, operations, and delivery of services. A Gender and Security Toolkit produced by several international organizations describes the type of comprehensive approach that is needed:



> Gender equality, inclusion and diversity are achieved through carefully designed and resourced human resources strategies and practices based on the principles of equality and non-discrimination to which states have committed in international human rights treaties. Starting with top-level leadership, managing the institution in a way that reflects principles of equality and non-discrimination, including the promotion of diversity, and ensuring that these are taken seriously sets the tone and indicates what is and what is not permissible. Leadership on gender equality not only moves downwards in the hierarchy, but ideally includes openness among senior management to inputs, suggestions and concerns of more junior staff. Accountability, disciplinary, complaint and oversight mechanisms concerning the security and justice sector also play critical roles in supporting inclusivity, non-discrimination and gender equality.[4]

3 *Guide on the Security of Major Sporting Events: Promoting Sustainable Security and Legacies*, UNOCT, UNICRI, UNAOC, ICSS, 2021, p. 183.
4 Security Sector Governance, Security Sector Reform and Gender, p. 23, in *Gender and Security Toolkit*, DCAF-Geneva Centre for Security Sector Governance, Office for Security and Cooperation in Europe (OSCE)/Office for Democratic Institutions and Human Rights (ODIHR), UN Women, 2019.

Gender equality and human rights must be woven into the organization's cultural fabric, through the creation of a respectful and empowering environment with clear procedures in place for preventing and dealing with sexual harassment and discrimination, both in the workplace and in interactions with the public. Staffing procedures must ensure and strengthen the participation of women in leadership and decision-making roles. It is also important to promote equality and inclusion in general and to recognize how gender intersects with race, ethnicity, class, religion, rank, and other factors. This also extends to members of the LGBTQI+ community, who often face discrimination, bullying, and harassment. This type of behavior cannot be tolerated toward anyone. It is up to the security planning leadership to create a safe, welcoming workplace and to communicate clear principles with all staff members, including through official mission and vision statements.

As with all human rights values, making equality and inclusion part of every process and practice is not only an international legal obligation; it also brings positive, practical benefits. It allows for a more comprehensive understanding of the security needs of the host community, expands the potential pool of talent to hire, promotes a more inclusive working dynamic within the organization, and improves community relations.[5] And it sets a good example. When the media spotlight shines on a major event, the public should be able to see a diverse security team that projects and promotes human rights, gender equality, diversity, and inclusion.

1.1.3 ENVIRONMENTAL SUSTAINABILITY

Another core value to uphold throughout the process is respect for the environment. The environmental impact of bringing together, housing, feeding, and moving hundreds or even thousands of security personnel over an extended period can be significant; on top of that are the physical structures that may need to be constructed and maintained to secure the various sites then dismantled after the event. This all takes a toll on the environment, which is why security planners need to do everything possible to reduce the operation's carbon footprint and adopt a green security posture. Host governments will likely promote broad policies to reduce greenhouse gas emissions associated with the event, in line with their commitments to address climate change, and security planning must take this aspect into account. It is important not only to follow local laws and public policies but to integrate the highest energy and environmental standards into every phase of the operation.

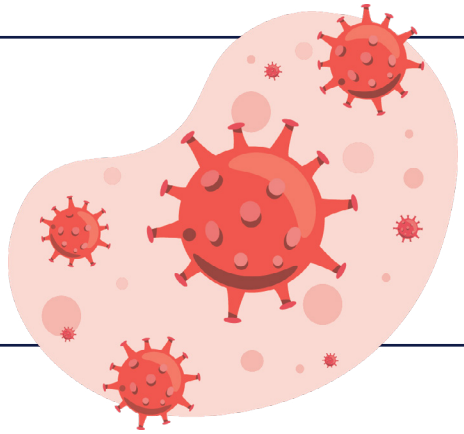
That process involves identifying areas of synergy between security and environmental sustainability objectives and finding effective ways to promote opportunities to increase sustainability—for example, by incorporating an environmental requirement into security supplier contracts. Minimizing the use of non-renewable resources, monitoring and analyzing energy usage, and reducing consumption are all steps that can be introduced in the pre-event planning stage and implemented throughout the entire process. The use of electric vehicles, biodegradable materials, reusable water containers, and recycling programs will all have a positive impact on daily operations and contribute toward a clean environment.

5 References and toolkits to assist security planners in integrating a gender perspective include the work of DCAF, OSCE/ODIHR, and UN Women, mentioned above, as well as the European Institute for Gender Equality's gender mainstreaming toolkits.

1.2 CROSS-CUTTING CONSIDERATIONS

1.2.1 HEALTH – COMMUNICABLE DISEASES

The COVID-19 pandemic has shown the dramatic impact a health crisis can have on major events around the world. The virus led Japan to postpone the 2020 Summer Olympic Games for a year, and many other international gatherings were reconfigured as virtual events, restricted to all but a few participants, or canceled altogether.



While the scale of the COVID-19 impact has been unprecedented, global health concerns have always been a factor to be considered for major events. These have sometimes caused widespread concern, such as with the outbreak of the H5N1 virus (avian bird flu) in 2006, prior to the Torino Winter Olympic Games in Italy; the H1N1 virus in 2010, prior to the G20 Leaders' Summit in Toronto, Canada; and the Zika virus epidemic in Brazil, in advance of the 2016 Rio Olympic Games. Delegates, spectators, athletes, tourists, or large contingents of the event workforce—including security personnel—could be negatively affected by any number of health concerns, ranging from localized food poisoning to a broader communicable disease, or even a natural disaster that causes an unexpected strain on the health system. These types of incidents can cripple security planning if proper contingency plans are not in place.

Security planners are generally not responsible for managing health emergencies at major events, but they do need to be prepared in case a health crisis affects their own personnel. They need to assess what kind of surge capacity they would have if a health crisis were to leave the workforce vulnerable or depleted, either during the event itself or in the months leading up to it.

The security workforce for a major event can number well into the thousands. The logistics around housing and feeding security personnel must include, among other things, health and safety plans incorporating food surveillance, isolation areas, and advance ordering of sufficient personal protective equipment (PPE).

The World Health Organization (WHO) cautions that preparation for a mass gathering should start early and include detailed planning and coordination.

> ***Planning and preparing public health systems and services for managing a [mass gathering] is a complex procedure: advanced risk assessment and system enhancement are critical to identifying potential public health risks, both natural and manmade, and to preventing, minimizing and responding to public health emergencies, WHO says.***[6]

The global health agency regularly produces and provides interim and permanent health guidance to host governments, health authorities, and national or international organizers of mass gatherings and major events. It has also developed specific guidelines in the context of COVID-19 which could also be useful once the health emergency has ended.

The impact of the COVID-19 pandemic highlights the importance for security planners to ensure that resilience-building measures and contingency planning for health crises and disaster recovery are factored into their preparations. Ongoing health risk assessments should be conducted in cooperation with the appropriate local, national, and international public health authorities. These are just some of the areas that WHO recommends need to be taken into account during a health risk assessment:

- **Characteristics of the event's designated venues (location, size, indoor/outdoor)**
- **Number and main characteristics of the expected participants in the event (age, health status, origin of travel)**
- **Expected interactions among participants during the event**
- **Expected duration of the gathering**
- **Other key features related to the specific event under consideration**
- **Any parallel or simultaneous event occurring within the vicinity that may create additional vulnerabilities**

WHO also provides support to government entities and international sport federations through a special unit dedicated to challenges associated with major events and mass gatherings.

6 *Public Health for Mass Gatherings: Key Considerations*,. World Health Organization, 2015, page p. 10.

1.2.2 TOURISM[7]

As in the case of health-related safety issues, tourism security does not necessarily fall under the mandate of security planning, but it is an area that requires policy coordination and alignment and presents opportunities for public-private partnerships. The short- and longer-term impact of a major event on tourism is a central consideration for local, national, and regional authorities, given the significant media influx and the potential to present a positive image. Quite often, international media outlets will venture beyond the event venue to cover stories focusing on local scenery, entertainment, history, customs, and traditions.

Of course, less positive aspects may also be of interest to the media, including criminal activity, dangerous neighborhoods, local law enforcement practices, and perception of safety. Enhanced cooperation between all public agencies and between the public and private sectors is therefore essential to protect people and property, particularly at locations regarded as vulnerable targets—places such as hotels, tourist attracts, recreational sites, markets, transportation hubs, and retail centers. By engaging and communicating with local tourism practitioners during every phase of the planning and operations, security planners may also be able to influence the longer-term security culture within the local tourism industry.

As an additional consideration, security planning for normal peak tourist seasons or, alternatively, for unexpected increases of visitors to a tourist destination may present organizational challenges and opportunities that are quite similar to those of major events. Therefore, the methodology explained in this manual can be easily adapted to tourism security.

1.2.3 CRITICAL INFRASTRUCTURE SECURITY

Critical Infrastructure consists of the physical and information technology facilities, networks, services, and assets whose failure or destruction would have a serious impact on people's health, safety, security, or economic well-being and the effective functioning of governments.

Ensuring the security and resilience of the country's entire critical infrastructure is a task well beyond the scope of the event security planners, but any disruption could have a major impact on the event. Therefore, security planners should open up lines of communication and engage in dialogue with the responsible authorities early in the planning process. Critical infrastructure security is a shared responsibility involving multiple stakeholders, because neither government nor the private sector has the knowledge, authority, or resources to do it alone. An effective critical infrastructure strategy should adopt an all-hazards approach to analyzing threats that include accidental, intentional, and natural hazards. Public-private partnerships are the foundation for protecting critical infrastructure security and developing effective resilience strategies, and timely, trusted information-sharing among stakeholders is essential.

7 See *Tourism Security in Mexico, Central America and The Caribbean 2016-2019: Key Findings and Recommendations*, OAS, UNICRI, 2019.

Some of the common types of critical infrastructure include:

Energy and utilities (for example, electrical power, natural gas, oil production, pipeline systems)

Transportation (air, rail, marine, highways)

Finance (banking, securities, investment)

Government (services, facilities, information networks, key national sites and monuments)

Manufacturing (defense industrial base, chemical industry)

Communications and information technology (telecommunications, broadcasting systems, networks)

Safety (chemical, biological, radiological, and nuclear safety, hazardous materials, search and rescue, emergency services)

Health care (hospitals, laboratories)

Food (agriculture, food industry)

Water (drinking water, wastewater management)

1.2.4 SOFT TARGETS/CROWDED PLACES

As with critical infrastructure, soft targets and crowded places (ST/CPs) are typically outside the direct responsibility of the security planning team for a major event, but they still warrant considerable attention. Any threat or attack on such a target within the host country will have a negative impact on the event and its corresponding threat level.

> Segments of our society are inherently open to the general public, and by nature of their purpose do not incorporate strict security measures. Given the increased emphasis by terrorists and other extremist actors to leverage less sophisticated methods to inflict harm in public areas, it is vital that the public and private sectors collaborate to enhance security of locations such as transportation centers, parks, restaurants, shopping centers, special event venues, and similar facilities.[8]

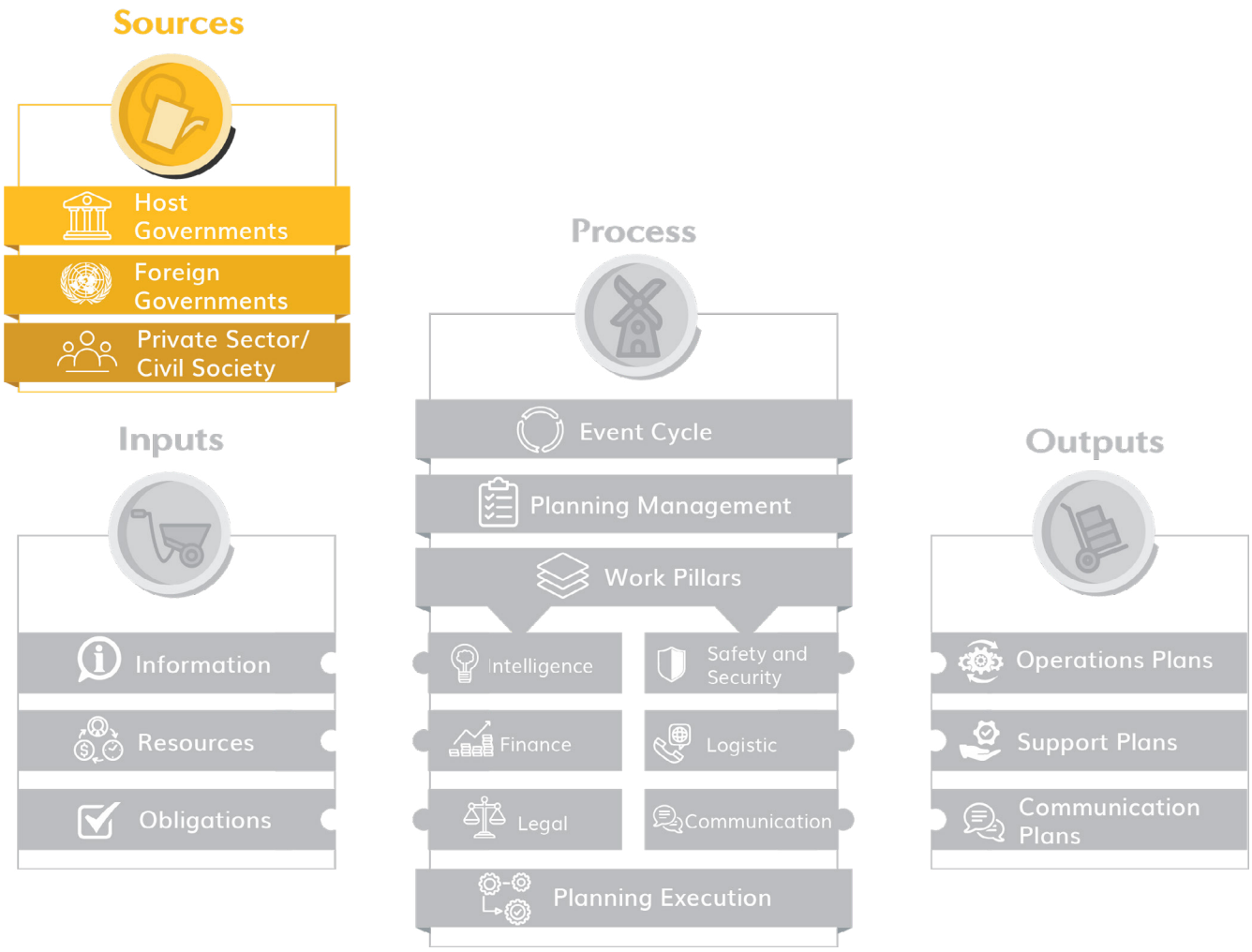
Even outside the venue of a major event, such targets may become more vulnerable as they draw large numbers of people unfamiliar with the site, the city, and maybe s the language. Therefore, it is paramount to consider all potential vulnerabilities which could arise and coordinate contingency plans with all potential stakeholders. The U.S. Department of Homeland Security has described this as a "shared mission."

> Reducing the risk of attacks against ST-CPs and reducing impacts of attacks that do occur is a shared mission among many stakeholders, including the general public; ST-CP owners and operators; security industry partners; State, local, tribal, and territorial (SLTT) government partners; and the Federal government. Individuals have a role within their community to help detect and prevent possible attacks against ST-CPs. ST-CP owners and operators have a responsibility to protect their sites and the people that work, use, or visit them. In addition to the critical role the security industry plays in directly securing ST-CPs and providing other security related services, the security industry also develops security related technologies and protective measures critical to the success of the overall effort. SLTT governments have the primary responsibility for preventing, protecting against, responding to, and mitigating incidents and attacks in their jurisdiction.[9]

Because of their complexity and the variety of stakeholders to be involved, planning the security of soft target and crowded spaces can also benefit from the methodology illustrated in this book, even when there is not a specific connection with a major event.

8 Cybersecurity and Infrastructure *Security Agency, Security of Soft Targets and Crowded Places–Resource Guide*, April 2019, p. 7
9 U.S. Department of Homeland Security *Soft Targets and Crowded Places Security Plan Overview*, May 2018, p. iii.

CHAPTER 2: SOURCES



The host government has primary responsibility for security policy and planning for any major event, through the coordinated efforts of multiple agencies, but it will invariably cooperate with foreign governments and other actors, primarily in the private sector and civil society, to ensure the event's success. In the parlance of the SIPOC diagram, these three groups of stakeholders are called sources. They generate the raw materials—informational, financial, and legal—that go into the security planning process.

At the very outset, it is important to have a clear picture of the agencies and organizations that must be involved in a complex undertaking such as security planning, in order to begin forging cooperative relationships. The earlier this can happen the better, to ensure that the various teams can mobilize their collective efforts and work together seamlessly as critical dates in the process approach.

Examining sources involves not only identifying the relevant agencies and individuals but also understanding optimum ways to interact, as well as the regulations and procedures that must be followed to obtain the desired inputs. This will lay the groundwork for effective cooperation.

Major events, in fact, create valuable opportunities for connection and cooperation among officials at the international, national, and local government level and members of the private sector and civil society. They allow for a productive exchange that can help reduce risk and add value and efficiency to the security and intelligence infrastructure.

Effective partnerships leverage different organizations' expertise and resources and provide complementary perspectives. They can also enhance communication, contribute to risk assessment, and improve program implementation. When selecting potential partners, it is important to look for a shared appreciation of the values discussed in Chapter 1, including high ethical standards, good governance, and respect for human rights and freedoms. These common values provide the basis on which to build strong relationships shaped by mutual purpose and trust.

2.1 HOST GOVERNMENT

Government security planners should begin with a thorough assessment of the internal sources with whom they need to interact throughout the planning process. A whole-of-government approach is required here. This means engaging the public sector's entire security and intelligence apparatus to make available as many national security assets, personnel, and equipment as possible. Starting with an inventory of internal sources and resources will make it easier to determine how to maximize the efficiencies and innovations of private enterprise, civil society, and academia and recognize the most critical areas for cooperation with foreign governments.

2.1.1 INTERAGENCY COOPERATION

Planners will need to establish an interagency mechanism to facilitate collaboration between government agencies and departments and between different levels of government. Interagency cooperation can be implemented at the local, regional, or national level and includes liaising with agencies responsible for overseeing the security of critical infrastructure. It "largely relies on a robust command and control structure with a clear delineation of leadership roles, decision-making processes, and responsibilities of each governmental agency in the early planning process."[10]

The following public ministries or offices are just some of the entities that typically coordinate with law enforcement agencies in security planning and preparation around a major event:

- **Health agencies, fire brigades, and civil protection authorities, to make sure that any type of contingency can be managed properly and that normalcy can be quickly restored in the event of a disruption;**
- **Local government authorities, to coordinate specific measures that may have an impact on security or public order, such as traffic, road and building maintenance, or street lighting;**
- **Foreign affairs, customs, and immigration authorities, as well as the consular or diplomatic corps of foreign countries, to handle specific issues related to the increased presence of foreign visitors;**
- **Judicial authorities, to investigate and manage the typically large number of cases surrounding a major event, involving either national or foreign citizens; and**
- **Ministry of Tourism or local specialized agencies, to coordinate matters that could have an impact on the hospitality sector.**

10 *Guide on the Security of Major Sporting Events – Promoting Sustainable Security and Legacies*, UNOCT, UNICRI, UNAOC, ICSS, 2021, p. 169.

2.1.2 NATIONAL MUTUAL AID

Many countries have national mutual aid networks or programs that allow agencies outside of a particular jurisdiction to provide support. These mechanisms ensure that local jurisdictions can call on partners in law enforcement, health, defense, and emergency services to assist with events or crisis situations that would otherwise stress or overwhelm local capacity. Many major events such as international sporting competitions or political summits would trigger the activation of such mutual aid instruments.

This is particularly relevant when multiple forces are responsible for different security elements or have different mandates or jurisdictions in relation to specific crimes or geographical areas, such as in the case of federal states or countries that have adopted decentralization policies for particular functions. Depending on the needs for a specific event, it is paramount to creatively and efficiently leverage the skills and assets of all these different sources to maximize the resources invested.

2.2 FOREIGN GOVERNMENTS

Major events often require cooperation between the host government and foreign governments or other international entities, to share intelligence, expertise, and information. Other countries that have hosted similar events in the past can be valuable sources of knowledge and experience for those involved in security planning.

The intelligence-sharing process for a major event often relies on pre-established formal mechanisms to securely exchange information with other agencies and countries. Event-specific memorandums of understanding (MOUs) or letters of agreement (LOAs) may also need to be signed prior to a particular event. This applies to all government and private sector partners sharing sensitive material. Planners should start early and allocate sufficient time to prepare the intelligence systems and infrastructure for cohesive collaboration. One option to consider is the establishment of an international fusion center, where host and foreign governments can meet physically or virtually to collect, process, and share intelligence.

In addition, foreign governments can provide or facilitate access to a wide range of resources and supplies which could be extremely helpful in implementing the security around a major event. Such resources may include specialized personnel or equipment, advanced technology, or financial support.

2.2.1 BILATERAL/MULTILATERAL COOPERATION

Many states have established bilateral or multilateral agreements that allow for direct cooperation with their counterparts in other countries. In many cases, existing mutual legal assistance treaties or international conventions facilitate ongoing formal collaboration. Security planners should review any such mechanisms that are in place, both to ensure that they understand any obligations arising from those agreements and are abiding by them as well as to explore the possibility of expanding the information and resources available.

Additionally, almost every major event involves the participation of other countries' citizens and representatives, whether they are visitors, athletes, or government dignitaries. In these cases, it is crucial to discuss, analyze, and consider each of the represented countries' specific security requirements and concerns in relation to the event, with a view to coordinating specific measures appropriate to the circumstances.

2.2.2 INTERNATIONAL ORGANIZATIONS

Cooperation with international and regional organizations should also be an early consideration for security planners. Within their respective mandates, several organizations have developed and are implementing specific programs to assist member states in the different phases of security planning for a major event. These include the United Nations Interregional Crime and Justice Research Institute, through ECOSOC Resolution 2006/28;[11] the United Nations Office of Counter-Terrorism, with programs on sport security and on the protection of vulnerable targets;[12] and INTERPOL, with its Project Stadia, which promotes law enforcement technical cooperation.

11 UN Economic and Social Council, ECOSOC Resolution 2006/28, "International Permanent Observatory on Security Measures during Major Events."
12 *Guide on the Security of Major Sporting Events – Promoting Sustainable Security and Legacies*, UNOCT, UNICRI, UNAOC, ICSS, 2021.

Several other UN agencies and international organizations are also equipped to offer technical assistance on one or more specific elements of security in the context of major events. These include, for instance, the World Health Organization for international health regulations, the International Atomic Energy Agency for nuclear security, or UN Women for an improved gender perspective.

Similarly, regional organizations may enable closer cooperation among member states and offer specific security programs geared toward major events. For example, the OAS Inter-American Committee against Terrorism has carried out a regional program on this topic since 2006. The Caribbean Community Implementation Agency for Crime and Security (CARICOM IMPACS) has also developed substantial efforts in this field, as have other organizations around the globe. These include the European Union, the Council of Europe, the Organization for Security and Co-operation in Europe, the African Union, the Association of Southeast Asian Nations, Asia-Pacific Economic Cooperation, the Commonwealth of Nations, and the *Organisation internationale de la Francophonie*, to name a few.

Moreover, most of these organizations plan and organize major events themselves, mainly political summits, and thus have developed and adopted clear mechanisms and protocols for international cooperation on security. Similarly, large sport federations and international organizing committees play a key role in facilitating international cooperation in relation to the events they are organizing. Event organizers should familiarize themselves with the plethora of resources available—including several referenced in this publication—to define what is most relevant and useful to their specific needs before proceeding with the development of the security plan.

2.3 PRIVATE SECTOR AND CIVIL SOCIETY

Security operations also depend on experts from outside the government or international organizations to provide specialized knowledge and leading-edge capabilities. Potential partners can come from the business sector, academia, or civil society organizations. Their expertise and technical know-how can complement official efforts and mitigate potential risks. The private sector also has extensive and established communication networks that can be used within the security team and for more widespread communication. Used effectively, these channels can help security planners disseminate critical information in a cohesive, timely, and efficient manner.

2.3.1 PUBLIC–PRIVATE PARTNERSHIPS

Public-private partnerships (PPPs) are increasingly important components for enhancing the security of major events. The opportunity to pool resources, experience, and information can result in valuable benefits. PPPs should be used to maximum advantage within the appropriate government, legal, and logistical parameters. One important caveat: Formal agreements and structured review procedures must be in place to establish clear guidelines, ensure an efficient operation, and avoid complications.

From a practical standpoint, several security aspects are often handled most efficiently and effectively in partnership with the private sector; these may include technology development and implementation, cybersecurity systems, hospitality services, or buildings and venues hosting the events. In all such cases, PPPs must be designed to identify effective solutions, and the rules around public procurement and competition need to be understood and respected. There is also the potential for the mishandling or misuse of information. Personnel trusted with sensitive or classified information should undergo a proper security screening and vetting process to help mitigate the risk of internal corruption.

For major sporting events, corporate sponsors offer another potential source for mutually beneficial partnership arrangements. Many corporate partners have their own security apparatus, which includes security practitioners and intelligence professionals who are often former law enforcement officers. Corporate partners also have material assets that they will often share in support of mutual security objectives. In addition to corporate sponsors, security managers and owners of event venues should also be included in the planning process.

Private security contractors are another source of valuable support. The scope and magnitude of most large-scale major events typically strain the capacity of public law enforcement agencies to meet the expected security level. The use of private security personnel, within proper parameters, creates a force-multiplying opportunity. "In developing operations security plans, the roles and division of tasks between private security and law enforcement must be clearly delineated, and constant information exchange between these stakeholders is a must."[13]

Several manuals have been developed at the international, regional, and national level to share best practices related to the establishment of PPPs and facilitate the use of the resources and information that the private sector can offer.[14]

13 *Guide on the Security of Major Sporting Events – Promoting Sustainable Security and Legacies*, UNOCT, UNICRI, UNAOC, ICSS, 2021, p. 90.
14 In 2009, UNICRI and the OAS created the "Handbook to Assist the Establishment of Public-Private Partnerships to Protect Vulnerable Targets" to support stakeholders with their public-private partnership efforts. They expect to produce a new handbook on the subject in 2022.

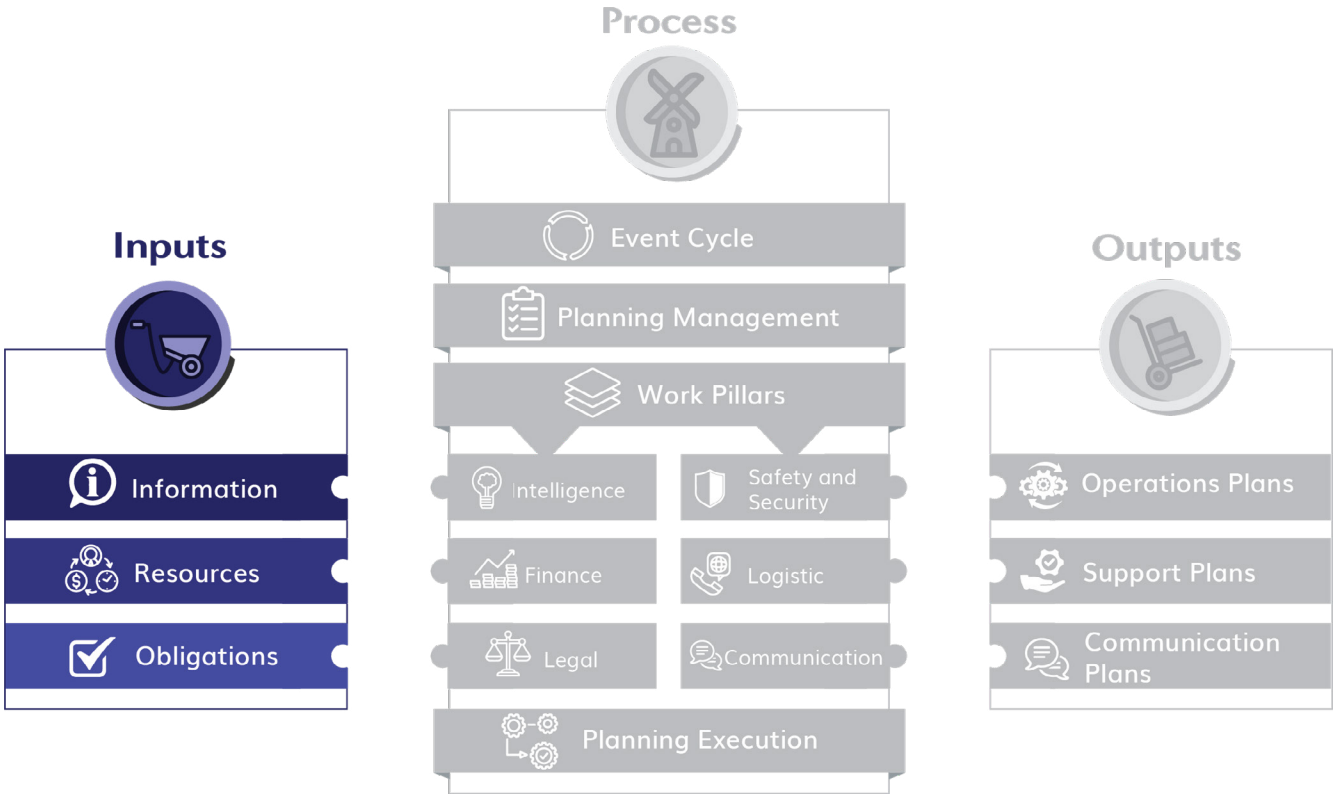
2.3.2 CIVIL SOCIETY, ACADEMIA, NONGOVERNMENTAL ORGANIZATIONS

Additional support for security planning may be found through universities, research institutes, and other academic bodies, as well as nongovernmental organizations (NGOs) or community groups operating in the host country.

These stakeholders can play an important role. For instance, an academic institution may be able to carry out needed research in advance of the event, develop a security model using artificial intelligence to predict possible challenges, promote initiatives to help create a general atmosphere of security, or develop volunteer opportunities for students to get involved in the event.

For their part, nongovernmental organizations and other members of civil society can become key partners in the implementation of security plans by promoting specific programs on crime prevention at the national or local level. With proper outreach and respectful engagement, members of the community may not only become a source of local intelligence, but also provide important perspectives and insights on issues such as human rights concerns or local community impacts. Building a solid relationship with civil society representatives and keeping them informed throughout the planning process will help to ensure the success of an event.

CHAPTER 3: INPUTS



This chapter looks at the inputs that go into the security planning process—in other words, the raw materials obtained from the sources laid out in Chapter 2. As explained in the Introduction, three general types of inputs go into any security plan: **information**, including intelligence; **resources**, whether human, material, or technological; and **obligations**, which include any relevant laws, regulations, protocols, or procedures.

These inputs may be available from any of the different sources discussed in the previous chapter, and part of the job of security planners is to analyze the options available and identify the most beneficial and effective. If the operation will require additional security personnel, for example, planners need to determine whether the situation calls for assistance from other jurisdictions within the country, whether a foreign government might be able to provide some consultants to supplement national expertise, or whether the use of some private contractors might be appropriate for specific tasks. Likewise, some technological capabilities may be available through a local university, while others may be obtained via a cooperation agreement with another government. All these decisions must comply with existing obligations, ranging from international treaties to national legislation to private contracts. And, as discussed in Chapter 1, all such decisions should be made in adherence to core guiding principles.

3.1 INFORMATION

Information is an essential commodity to plan and deliver the security for a major event. It is impossible to begin planning without a clear understanding of the event itself and the expectations of the event organizers.

3.1.1 GOOD PRACTICES AND LESSONS LEARNED

Security planners, no matter how experienced, need to study as much as possible about the security situation surrounding similar events held in the past. This background information, together with current data, will give them a clearer picture of the context. Even if every major event is unique, it is important to be aware of good practices that have been developed and carried out in similar circumstances. Gaining access to this knowledge will require effective channels of communication and knowledge transfer with other countries and organizations. Just as importantly, planners must develop specific skills to assess which good practices and lessons learned may be applicable, what can and should be adapted, and what is not relevant to the current situation.

3.1.2 EVENT-RELATED INFORMATION

Leading up to and during a major event, a fluid, timely, and ongoing exchange of information between the event organizers and the security planners will strengthen the plan development process and enable the efficient sourcing of required equipment and materials. Security planners must be constantly advised of all program details related to the event and any updates, additions, cancelations, or changes, big or small. An intake process should be established to collect, log, and disseminate information received by the security planning team. Information should be available as appropriate to all planners via a shared records management system with a mechanism to alert all users in a timely manner to enhance their situational awareness. Information can come in many forms (for example, verbally or in print, through news broadcasts, articles, communiques, or social media) and from different origins (such as the event organizing committee, the Internet, partner stakeholders, or members of the public). The sources identified in Chapter 2 will be both suppliers and receivers of much of the information required for the security of the event.

3.1.3 INTELLIGENCE

Information becomes intelligence once it is collected, analyzed, and interpreted specifically for security purposes. In the SIPOC approach applied here, the data is an input that feeds directly into the intelligence workforce pillar of the planning process. The intelligence produced as a result assists planners and operators in identifying and preparing for potential risks and taking action to support the security of the event and the surrounding community. Chapter 4 will discuss the production and sharing of intelligence in more detail.

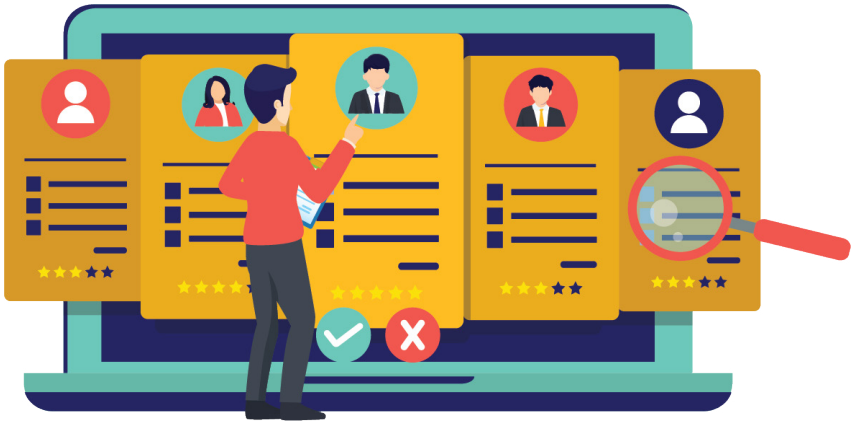
3.2 RESOURCES

Any major security undertaking requires considerable resources to be able to promptly and efficiently respond to the mission requirements, needs, and challenges. Part of the security planning process involves assessing the human, material, and technological resources that will be required and determining where these can be obtained. The host country, including local government agencies, will be responsible for supplying the bulk of the resources; however, all the sources identified in Chapter 2 can contribute as needed and as appropriate, depending on the relationships, legal agreements, or types of cooperation in place.

3.2.1 HUMAN RESOURCES[15]

In the case of most major events, a large workforce—sometimes numbering in the thousands—will be necessary to plan and deliver safety and security. Large contingents of law enforcement, military personnel, private security officers, consultants, administrators, support staff, and volunteers will be required to maintain the security posture in the lead-up to and during the event. The resourcing of personnel should be a shared responsibility drawing from many of the sources identified in Chapter 2. Decision-makers must understand the complexity of security planning and the need for input from experienced, skilled people representing different stakeholders at each phase of the event: planning, mobilization, operations, and close-out.[16]

The functional components of the security workforce will need to be defined with specific terms of reference (ToRs) to describe mandates, delineate clear roles and responsibilities, and ensure accountability. Experience has shown that the placement of untrained and inexperienced planning personnel in these positions risks system breakdown and leads to increased stress, lack of management confidence, and a failure to meet critical deadlines. For these reasons, planners should give serious consideration to providing training focused on planning principles and staffing requirements for the specific event, to ensure an understanding of roles, responsibilities, and expectations for both public and private security personnel.



It will be essential to identify how many personnel will be needed and when, as well as the level of expertise required for leadership and management roles. Identifying, selecting, and training sufficient skilled personnel for the operational phase will be a significant task requiring considerable coordination from a planning perspective. The recruitment of both salaried staff and volunteers is managed by the lead security agency—the security organization or law enforcement agency that assumes responsibility for the overall security of the event and is accountable for all aspects of security planning.[17] Security personnel should come from the respective government departments, supplemented by private security contracts if necessary. The national police service and military will usually provide significant numbers of security officers, drawing on support from regional and local police services. Consideration should also be given to enlisting the services of other law enforcement entities such as coast guard, park rangers, conservation officers, fisheries officers, or any other national, regional, or local law enforcement professionals, to enhance the security complement and create a force-multiplying effect.

15 The issue of human resources is discussed further in Section 5.2.1.1 of this manual.
16 See Chapter 4.1.1 of this manual on the planning phases for an event.
17 See Chapter 4.2.5 of this manual.

3.2.2 MATERIAL RESOURCES

Significant assets are required to support the security of the event. First, there is the physical security equipment such as fencing, lighting, CCTV cameras, alarm hardware, metal detectors (structural and handheld), warming huts, cooling stations, medical supplies, fire suppression gear, and explosive detection devices. Security planners will also need to procure or ensure the availability of a host of additional assets such as vehicles (cars, buses, trucks, bicycles, boats, motorcycles, 4x4s), personal protective equipment (PPE), and personal sundries for personnel, such as sunscreen, insect repellent, water, and snacks, to name just a sampling of the inventory that may be needed. The type of event and location will determine the exact assets necessary for the event. A secure tracking system using barcodes, QR codes, or RFID technology will be needed to distribute, track, and recover returnable assets issued for temporary use.

3.2.3 TECHNOLOGY

The efficient use of technology can be a force multiplier and cost-effective way to supplement safety and security measures. Technology can enhance the surveillance footprint and reduce human resource requirements as well as reduce physical stress on an often limited and stretched workforce. The key is to ensure seamless interconnectivity to be able to communicate and share data across different systems and technologies.

Data can come from many sources, including surveillance cameras, video analytics technologies, open-source information, public data banks, utility and transportation companies, emergency call centers, access control and alarm systems, and simulation software, to name a few. Highly integrated systems will enable all these data points from multiple streams to be aggregated into real-time information for security planners and operators. Experienced planners can also use technology to mine information that is publicly available on social media for troubling keywords and any indications of potential threats. Technological advances in areas such as artificial intelligence, facial recognition, biometrics, and deep learning can be considered when exploring security options, always respecting and adhering to legal requirements and international standards.

3.3 OBLIGATIONS

Any of the sources involved in security planning for a major event will require stakeholders to follow specific rules and regulations, protocols, or procedures. These can be defined as the obligations planners need to take into account when organizing an event and working with different levels of government, the international community, or private companies alike.

3.3.1 NATIONAL LEGISLATION

All steps of security planning should be executed within robust legal and institutional frameworks that facilitate the effective and efficient fulfilment of all security requirements.[18] To this end, host governments must ensure that all relevant matters are covered by adequate, clear laws and regulations and that relevant actors understand their obligations and are aware of any legal resources available to help them overcome the multiple challenges of a major event.

Depending on the event and the context, security planning invariably involves dealing with specific situations, such as having to close the airspace above the event venue or needing to develop ad hoc procedures to manage human resources. These actions may be covered under the existing public security framework; if not, the host country could seek to amend certain laws, such as those adopted to counter terrorism or ensure public order, or develop special laws that apply to issues related specifically to major events. Creating a template for new legislation will require making a careful inventory of the main elements needed and becoming familiar with good practices and model legislation developed by other countries for similar events.

As part of this process, governments need to be mindful of international standards and requirements and carefully evaluate the impact of legislative measures on all participants involved, as well as the impact of technology and use of force.

3.3.2 INTERNATIONAL REQUIREMENTS

Modern international instruments related to the security of major events contain safeguards requiring states to comply with treaty obligations on human rights. International organizations have also developed standards devoted to promoting gender equality and fighting racial discrimination, xenophobia, and other forms of discrimination. Certain instruments also address the protection of human rights in a counter-terrorism context. Some examples include Human Rights Council Resolution 35/34,[19] and the reference guide *Conformity of National Counter-Terrorism Legislation with International Human Rights Law*.[20] Event organizers and authorities responsible for security must embrace these standards to ensure accountability among all stakeholders, including law enforcement. Host governments must not only comply with their obligations under international human rights law but conduct prompt investigations into any alleged breaches.

18 *Guide on the Security of Major Sporting Events: Promoting Sustainable Security and Legacies*, UNOCT, UNICRI, UNAOC, ICSS, 2021, p. 49.
19 Resolution 35/34, "Protection of human rights and fundamental freedoms while countering terrorism," adopted by the UN Human Rights Council in 2017.
20 This reference guide, published in 2014, is an initiative of the United Nations Counter-Terrorism Implementation Task Force (CTITF).

Human rights standards are not the only international obligations that have an impact on security planning. It is extremely important to comply with the full range of obligations deriving from international agreements. Some of these are strictly related to security matters, such as in the case of airport security, passport control, and customs measures. Others may not seem directly related to security but can have a big impact in certain situations if not carefully considered; these include issues involving judicial cooperation and extradition, international protocols and regulations for payments in foreign currency, or international licencing matters.

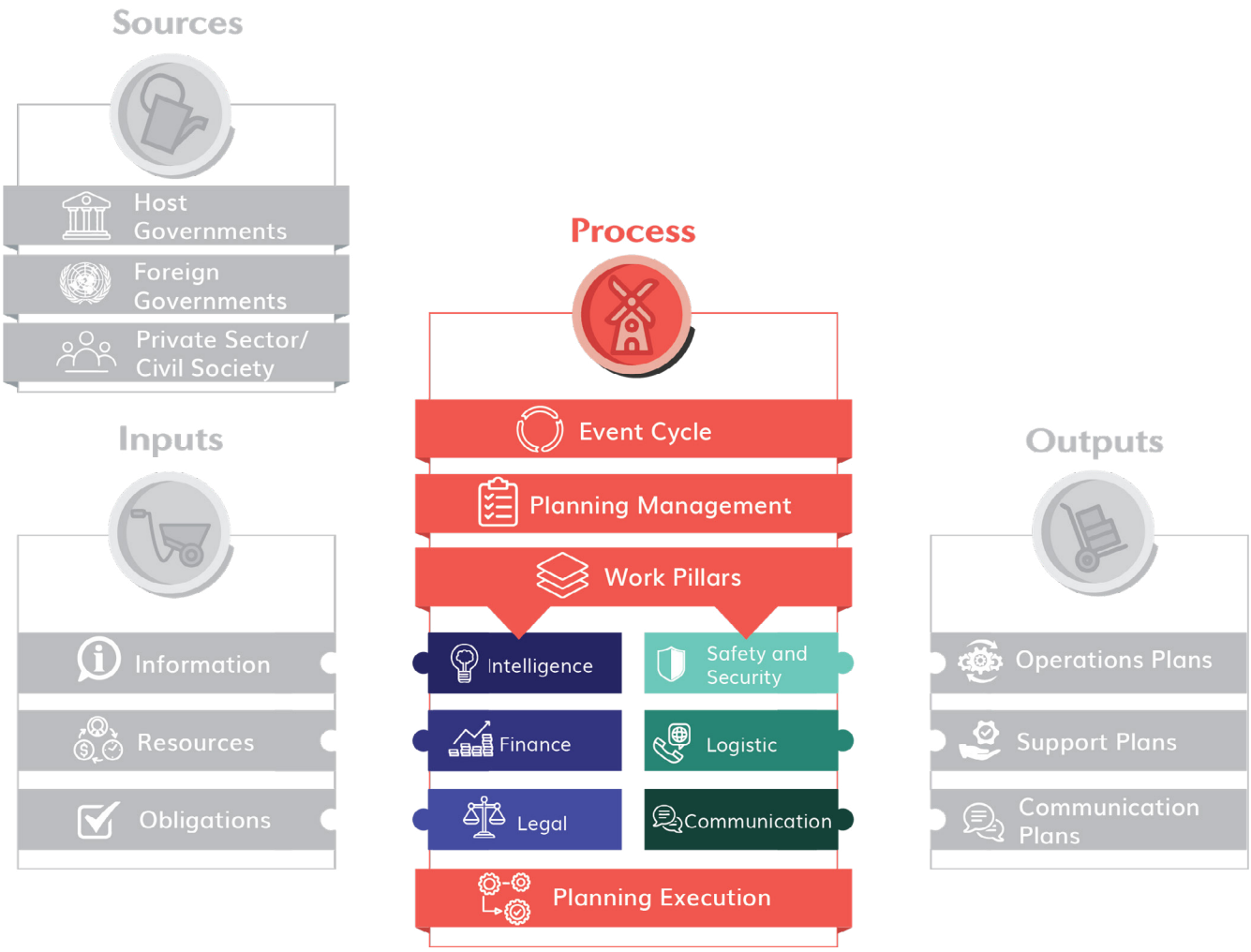
Proper security planning for any major event necessitates a careful assessment of all rules, regulations, and agreements deriving from international organizations or associations, as well as bilateral or multilateral agreements with other countries.

3.3.3 PRIVATE CONTRACTS

As explained above, the security planning process for a major event requires a substantial amount of human and material resources, including armaments and equipment, surveillance technology, buildings, infrastructure, and vehicles. The host government alone will not always be able to meet all the needs. Security planners must understand all the options available and take informed decisions to enable the efficient implementation of event security. This often entails partnering with private actors at the international, national, and local level.

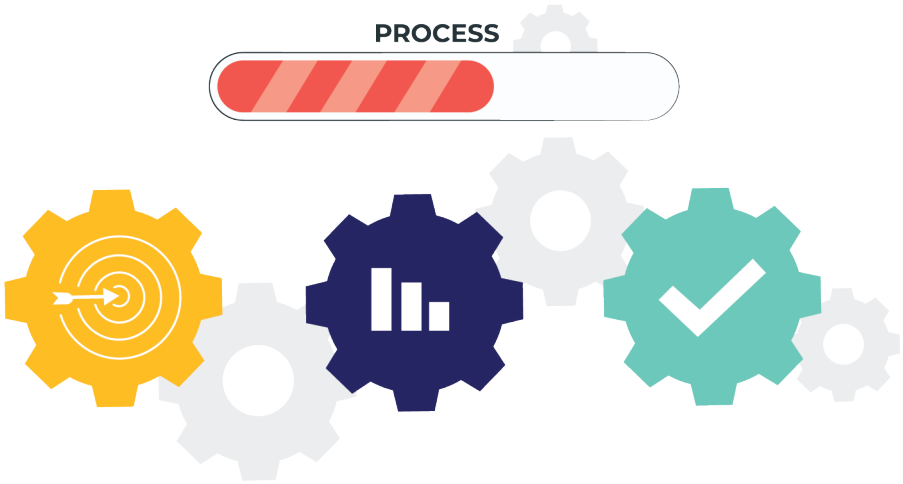
When working with the private sector, host governments must adopt an open, transparent, and competitive procurement process, accompanied by robust auditing and public scrutiny measures, and must ensure that the resources employed meet all applicable national and international requirements. Contracts must lay out high standards and enforce compliance with regulations on the role and accountability of private companies—including those providing security services—and on their relations with the host government or with security planners.

CHAPTER 4: PROCESS



Security planning for a major event is such a massive, complex undertaking with so many players and moving parts that planners need to create a reliable structure for engagement among senior government planning officials, event organizers, and private sector partners. Close collaboration will be essential to accomplish goals and overcome any number of difficulties that may have an impact on the creation or execution of a security plan. The challenges that the lead security agency must consider include focusing multiple partners on a common mission, identifying resource requirements, and building and operationalizing a sustainable planning system.

The process component of the SIPOC model comprises all the actions taken in the context of security planning, from identifying sources and developing inputs to transforming those raw materials into outputs—in other words, the final plans. This chapter examines the different steps of the process, from the earliest planning phase to the after-action review, and discusses what goes into successful planning management and how to organize the workforce.



4.1 THE EVENT CYCLE

4.1.1 PLANNING PHASES

Depending on the size and scope of the event, the location, and the resources available, security planning for a major event can take several months or even years. During this time, many unforeseen events can cause the planning team to lose focus and fall off track. Dividing planning requirements into phases, each with its associated activities, can help organizers keep their sights on what must occur before, during, and after the event.

Major Event Primary Planning Phases

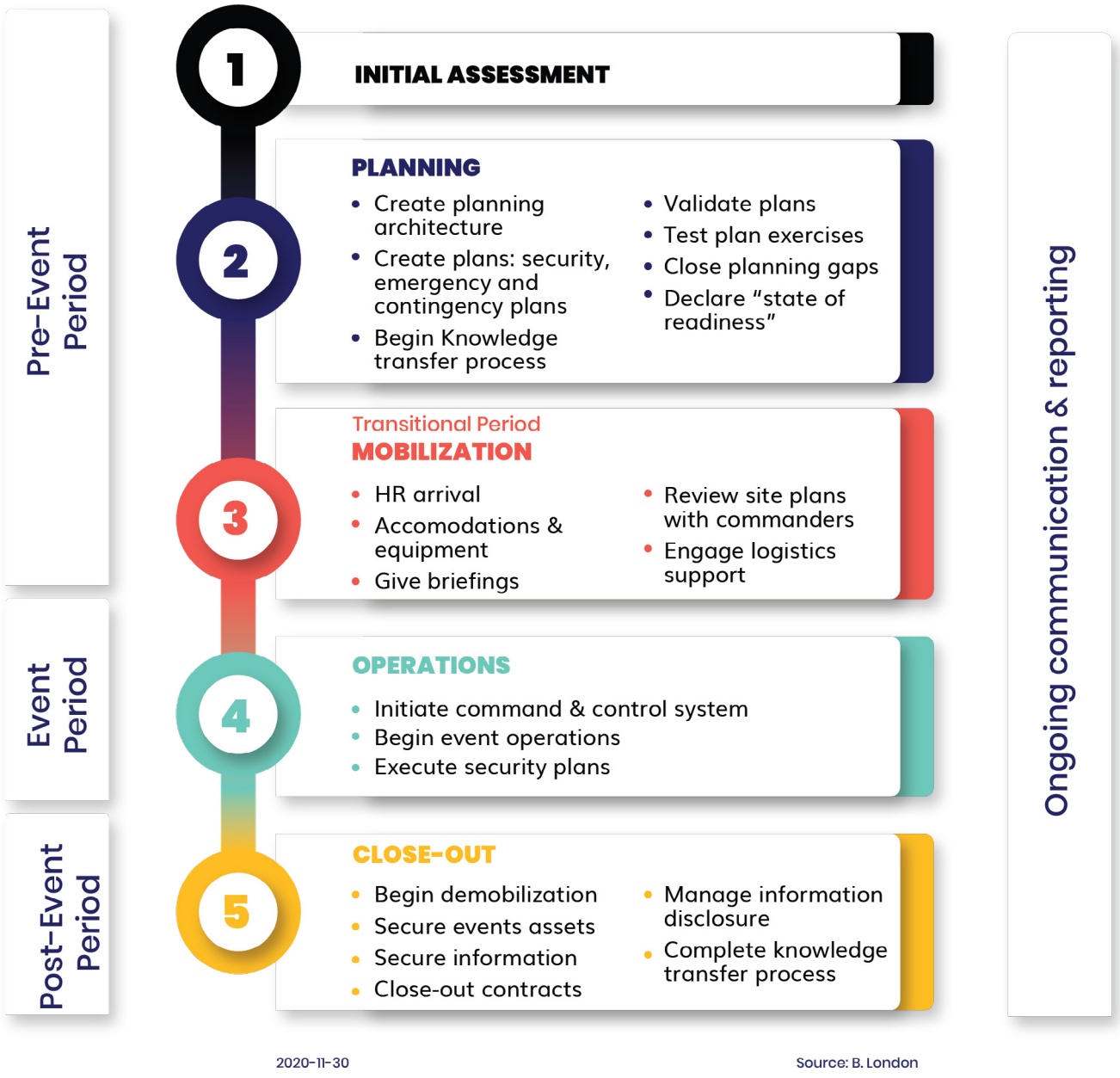


Diagram 3[21]

21 Developed in the context of the *Guide on the Security of Major Sporting Events: Promoting Sustainable Security and Legacies*, UNOCT, UNICRI, UNAOC, ICSS, 2021.

The **planning phase** is the longest and most complex part of the process. It is useful to do an initial assessment to better understand the main challenges and opportunities ahead and the potential impacts of a range of internal and external factors. A SWOT analysis—the acronym stands for strengths, weaknesses, opportunities, and threats—can provide a good internal evaluation at the outset of the process. A PESTEL analysis looks at the macro level and assesses how different external factors—political, economic, social, technological, legal, and environmental—could affect the organization and the planning process. Additional early steps include identifying potential stakeholders, defining and assigning the roles and responsibilities of everyone who will contribute to the security plan, and entering into contractual agreements or memorandums of understanding. During the planning phase, it is helpful to have a model that visually depicts the high-level components of the process, including a timeline that identifies the critical milestones necessary for success. Depending on the nature of the event, this phase will also include threat and risk assessments which will ultimately shape how security plans evolve. It is also recommended that planners set up knowledge transfer procedures which will be in effect throughout every phase; this often-overlooked step enables the team to collect information about what worked and what did not. Other activities are listed in the diagram above.

The **mobilization phase** iis a transitional period that occurs just before the event, following the declaration of a state of readiness. This can be a time of increased pressure for planners. It is when the security force is mobilized and material assets are put in place to support the operational security requirements. A large number of personnel must be accommodated in terms of transportation, sleeping quarters, meal areas, and equipment. Commanders must be briefed and must familiarize themselves with the operations and contingency plans.

The **operations phase** is when the command-and-control mechanism is implemented, meaning that the operation is now under the authority of one designated individual or a command center. The security provisions are in place, and it is time to execute the operations plans. This phase may last from just a few days to several weeks, depending on the duration and nature of the event.

The **close-out phase** immediately follows the event. The planning cadre remains in place to manage the close-out process. The demobilization of the security force takes place at this time and must follow the prescribed demobilization plan in terms of human resources. It is a period when assets must be secured and returned to their source, contracts closed out, and requests for information answered. It is also the time to collect and analyze the data obtained through the knowledge transfer arrangements—this will serve as an important resource for the after-action reports discussed below—and for evaluating the process and assets. This phase may last anywhere from months to years, again depending on the nature of the event. It is important to establish a robust and ongoing internal communication process throughout all these phases.

4.1.2 EXERCISE PLANNING

During the planning phase, organizers will have developed numerous operations and logistics plans among multiple security partners. No matter how detailed or well-designed, plans are of no value if they cannot be operationalized or executed. Exercise testing provides a way to assess the effectiveness of plans and offers an opportunity for those responsible for plan execution to improve their capabilities and readiness. It is advisable to make time to test the plans during the planning phase. Conducting a series of drills or exercises will help determine whether the plans will work and will make it easier to identify operational gaps. A point person should be appointed to track the necessary changes and close the gaps; this change control coordinator would work with each of the six work pillars to ensure that all the various aspects are aligned. The exercise testing process will indicate the plans' operational state of readiness. It is the exercise planning team's responsibility to design the type and format of the testing requirements and then produce a timeline of when each will be implemented throughout the planning phase. Exercises can take the form of table-top discussions or full-scale live drills with all the partners responding to simulated scenarios.

4.1.3 COST-BENEFIT AND OPTIONS ANALYSIS

For any country staging a major event, the primary focus of the security scheme will of course be to protect people and property. That often demands a significant investment. Prior to the event, it is important to assess the planning strategy from the standpoint of its socioeconomic impact. Assessing costs and benefits and weighing different options can inform policy planning and educate decision-makers about potential opportunities, possible negative consequences, and expected financial impacts.

Assessing costs and benefits and weighing different options can inform policy planning and educate decision-makers about potential opportunities, possible negative consequences, and expected financial impacts.

From a security planning perspective, the development of effective prevention and response options— particularly those involving technology, equipment, and systems—will require a clear-eyed analysis at every level to promote the wisest use of resources.

- **At the strategic level: What resources need to be procured or allocated, and why?**
- **At the tactical and technical level: What is the required capacity, specification, and scope of the needed resources?**
- **At the operational level: How can resources best be deployed to maximize the return on investment?**

Instilling a culture of rigorous analysis can improve the management of scarce resources and ensure accountability to taxpayers. The assessment process also leads to other types of added value, including:

- **Better identification of strategic operational objectives, ultimately enabling a more accurate assessment of performance;**
- **Effective management and use of available technical, human, and financial resources to avoid wasteful security spending and duplication of efforts;**
- **Delivery of cost-effective and robust security response options;**
- **Structured testing of implementation, allowing for better assessment of applicability elsewhere;**
- **Standardization of tactics and training; and**
- **Opportunities for interoperability, equipment sharing, and the development of networks for the exchange of best practices.**

A deeper cost-benefit or options analysis may also take a broader view to consider the potential longer-term impacts of security measures on the lives and socioeconomic circumstances of local communities, businesses, and the public as a whole. By seeking ways to enhance positive aspects and reduce adverse ones, benefits will accrue far beyond the event itself.

4.1.4 AFTER-ACTION REVIEW AND POST-EVENT EVALUATION

After the event, it is essential to conduct a structured, professional after-action review to objectively analyze outcomes and identify areas for improvement. The aim is to compare *intended* versus *actual* results; consequently, a thorough cost-benefit assessment from the outset is essential to help objectively define what was intended.

The after-action review evaluates the security planning process by asking some basic questions:

- **What was planned?**
- **What actually occurred? (This calls for facts, not subjective judgments.)**
- **What went well, and why?**
- **What could be improved, and how?**

These types of reviews can be wide-ranging or narrowly focused, but a wider perspective is likely to be the most productive in terms of organizational learning. The key to success is to insist on openness, honesty, and active participation regardless of the participant's rank, status, or position. If conducted in a constructive spirit, with unbiased facilitation, the process will highlight deficiencies, pinpoint ways to sustain strengths, and put the focus firmly on improving performance in the future.

There are different ways to organize after-action reviews. In some cases, the focus might be on key incidents, themes, or issues. Alternatively, a chronological review is often easy to structure, and participants may more easily recall what happened if the review follows the actual sequence of events.

A blended approach draws on both chronological and thematic elements. The outcomes identified in the discussion process can be integrated and analyzed with supplementary information gleaned from written evaluations, surveys, statistics, and other event-related reports, for instance.

The use of evaluations and analyses need not be confined to the start of the planning process or the conclusion of the event. In fact, reviewing progress and analyzing options throughout the process can identify gaps along the way and enable planners to correct course if necessary. The longer-term value of this process will rest on factually and objectively recording the outcomes, applying the lessons learned, and sharing the results when appropriate.

4.2 PLANNING MANAGEMENT

4.2.1 LEADERSHIP

Security planning for a major event requires a leadership balancing act. Given the complexity of the event and the number of stakeholders involved, effective leadership is essential. The lead security agency must have a team headed by someone who is accountable to deliver on the plan and can maximize the effectiveness of the multitude of agencies involved. Managing the different expectations of the government, the organizing committee, and security and private sector partners can be difficult.

Experience has shown that two contrasting leadership styles, relationship-oriented and task-oriented, are necessary parts of this leadership function. Here is an apt description of what it takes to lead a security planning effort:

The key to success is selecting a leader with proven skills in building relationships and trust in colleagues and partners. [...] The three elements of trust are capability, competency and caring. Followers should clearly see each of these components in the leader. A characteristic of strong trust is vulnerability. A leader must create a safe environment where followers know they can be vulnerable, seek assistance if they need it, not take on unmanageable risk and be open to constructive feedback. When a leader creates this type of environment it will result in commitment and accountability on the part of the security team.

The leader must be authentic and possess emotional intelligence. Emotional intelligence, at its core is the capacity to be aware of our emotions and consciously use them, to be aware of others' emotions and the ability to manage ourselves effectively in relationships. Emotional intelligence is widely accepted by private and public organizations as an essential element for leadership success. In the complex multi-agency environment of major event security, emotional intelligence is essential. [...]

Security planning for a major event will be challenging and at times stressful. Trust in the leader and strong morale will assist in overcoming many of the challenges.[22]

4.2.2 GOVERNANCE

Lessons learned from previous events demonstrate how critically important it is for a large, complex planning organization to have a system of good governance to ensure that its members follow the established process, policies, and operations. Good governance embodies the values discussed in Chapter 1, including respect for diversity and culture, the protection of human rights, gender equality, inclusiveness for people with disabilities and members of the LGBTQI+ community, and a sustainable environmental approach.

Accountability and oversight are an absolute must to fulfill the desired mission. The governance model needs to be aligned with the security mission statement (see below, 4.2.3). In the context of security planning, a proper governance model:

- **Includes measures to monitor and record what happens;**
- **Takes steps to ensure compliance with agreed-upon policies and strategies; and**
- **Provides for corrective actions in situations where rules have been ignored or misconstrued.**

22 From unpublished advice provided to the authors of this report by Alphonse MacNeil, Assistant Commissioner (Retired), Royal Canadian Mounted Police. Officer in Charge, Integrated Security Unit – 2010 G8 and G20 Summits.

Effective governance models must first be established, understood, and agreed upon by all participants. In the absence of a good governance model, systems are doomed to break down and strategies and timelines are likely to be missed. This is because of the complexity of a major event. In many cases, the event will overlap jurisdictions; for example, event sites and critical infrastructure can span diverse geographical areas and even extend to other countries. Within the host country, the security planning team will tap into expertise throughout the government. These types of situations add a degree of difficulty, as the lead security agency often has no legislated authority over other agencies involved.

Therefore, to ensure compliance, it is essential that the participating agencies agree on a specific model of governance. It then becomes a management role to ensure the implementation of sound principles in terms of security planning.

4.2.3 STRATEGIC DIRECTION

When organizing a major event, planners must understand what they are trying to achieve in terms of the outcome or end state. The high-level blueprint for the outcome is commonly referred to as the mission statement. The lead planner, in consultation with all other relevant stakeholders, needs to formulate a mission statement and the strategic planning objectives required to achieve mission success. Developing a well-defined and clear mission statement is the first step to identifying the strategic direction the planning will take.

The mission statement will guide the workforce throughout the different phases of planning.

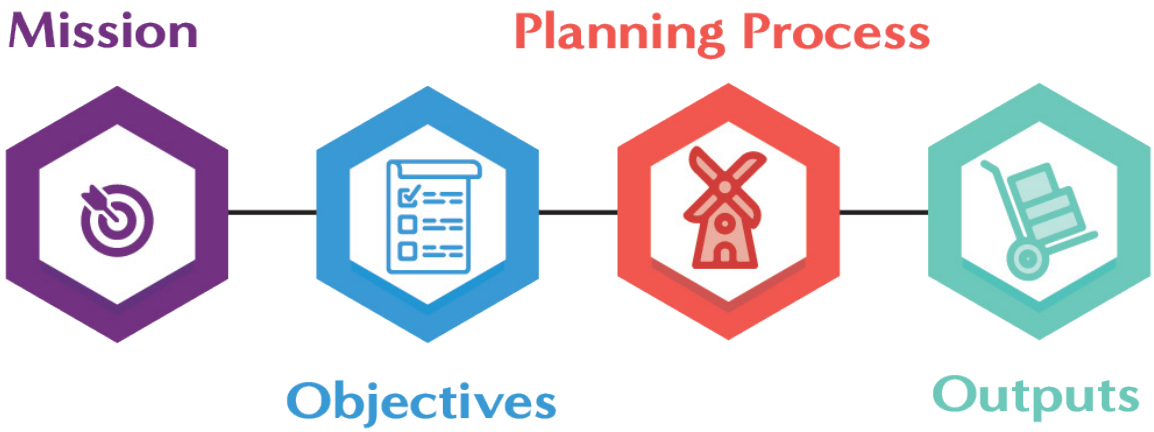


Diagram 4

4.2.4 PROJECT MANAGEMENT

The task of security planning in an ever-changing environment requires strong, flexible, and solution-oriented leadership and effective management. Lead planners or project managers must ensure that plans are developed, with the involvement of the lead security agency and its partners, to meet critical timelines and work together as a seamless operation.

Throughout the planning and close-out phases, management will need to coordinate meaningful, ongoing collaboration between the various pillars of the operation (described below) to ensure that everything is on track. The priority is to identify what each pillar needs to function and acquire the necessary resources to make sure all pillars are ready to operate and work together.

The lead planner must have experience in strategic planning, risk management, and performance management and must understand project management principles in order to direct the security planning process in line with the established governance model, through an organizational command structure. The use of internationally approved project management principles implemented by a professionally qualified project manager will ensure that planning follows a tried and proven process and provides structure to the decision-making. This approach should consider nine central aspects of the project: integration, scope, time, human resources, quality, cost, communications, risk, and procurement.

4.2.5 LEAD SECURITY AGENCY

The lead security agency is usually appointed by the host country's government ministry responsible for the event. This agency will be accountable for all aspects of security planning, which will be carried out under the event security director. Although the planning process is integrated, the lead agency is responsible for developing, maintaining, and overseeing the functional activities of the security planning system. It engages the various security agencies and stakeholders that handle the planning, operations, and close-out phases of the event.

The security agencies with jurisdiction over aspects of the event will normally align their planning structure to that of the lead security agency to produce a better coordinated and more efficient planning environment. The leads of each of these agencies, along with the event security director, form the event senior management team, while the six pillar leads will engage with their respective counterparts.

4.3 WORK PILLARS

An organized workforce is central to the ability to develop and implement security strategies for a major event, as it ensures that the human resource capabilities and system requirements are all in place and that the lead security agency can efficiently tap into the expertise at its disposal. Most security planning structures are organized around six common functions:

Each of these six pillars is crucial to the planning effort.

A well-defined and adequately resourced work pillar must be assembled and divided among the six pillars in order to make the security planning process operational. Given the complexity and magnitude of the event, each pillar should be led by someone from the lead security agency who has knowledge and experience relative to the pillar mandates. The pillar leads, as they are commonly called, report to the event security director. Below is a framework that has been successfully used to define and organize work functions into distinct pillars and planning cells for major events.

Three of these pillars—covering intelligence, financial, and legal matters—are mainly devoted to receiving and processing the inputs received by the sources. The other three—safety and security, logistics, and communications—contribute to the design and implementation of the outputs, in other words, the final security plans.

4.3.1 PILLAR 1: INTELLIGENCE

The intelligence pillar processes the information input and is critical to understanding threats and assessing risk. In receiving information from the different sources, this pillar will prioritize assets and determine the relative intensity of security operations across the entire footprint of the event.

International cooperation is crucial to delivering safe and secure events as it multiplies the number of sources for the information that the planners may receive. Host governments should maximize their existing national and international intelligence and law enforcement networks in support of the event security platform. Going through well-established global, regional, multilateral, or bilateral intelligence-sharing communities not only enhances security efforts for the event but strengthens collaborative relationships that support ongoing national security efforts to counter terrorism and combat organized crime. The multinational nature of many major events creates an opportunity to engage the participants' government security agencies to assist in the safety of their citizens and that of their world neighbors.

And cooperation can go beyond governments. As the *Guide on the Security of Major Sporting Events* puts it,

> ***"Although the official Government intelligence networks are the foundation of the information collection and distribution, the value and depth of the private-sector and corporate intelligence capabilities should not be underestimated and should therefore be sought after."*** [23]

In short, operations planning for a major event is by its nature intelligence-driven, and it is thus crucial to tap into all sources of intelligence available.

The creation of a joint intelligence group (JIG) is recommended to manage this pillar. Such a group would include representatives from relevant national, regional, and local law enforcement and government agencies. The group's mandate is to collect, collate, analyze, and disseminate accurate information and intelligence in a timely manner to facilitate the decision-making process in both the planning and operations phases of the event. The joint intelligence group must tap into any sources that are available, including open-source information (the press and social media), the general community, and even covert operations if necessary. Plans should be developed, and adapted as required, based on the most current intelligence, using a risk-based approach.

The joint intelligence group is also responsible for reviewing all threat and risk assessments conducted of the event sites to ensure that they include the most recent and accurate information that could have an impact on security at a specific location. It is the JIG's responsibility to produce a variety of analytical reports—covering tactical intelligence, strategic intelligence, threat assessments, and other information—on an ongoing basis. These reports will allow planners to produce flexible and adaptable plans that will enable commanders to adjust tactics to changing circumstances.

23 *Guide on the Security of Major Sporting Events: Promoting Sustainable Security and Legacies*, UNOCT, UNICRI, UNAOC, ICSS, 2021, p. 103.

4.3.1.1. INFORMATION MANAGEMENT

Information management systems are critical to the planning, implementation, and post-event phases of the event. Integrated planning requires organizational integration and, optimally, integration of information management and technology systems. During large-scale multi-partner security planning, it is important to initiate strategies that demonstrate how the different partners will work together and share information. Common databases are needed to manage plan development and handle asset management, mobilization, accommodations, transportation, and meals.

Depending on the governance structure and assigned roles and responsibilities, planners must also be able to accommodate post-event information requests from governments, police or security oversight agencies, the media, or others. All this raises practical considerations:

> The interface of computer and telecommunication networks significantly increases internal communications and information-management capabilities. The assessment of property space needs in terms of office space, furniture, transportation, and accommodation is an additional resource requirement.[24]

When selecting a technology solution, the relevant decision-maker should:

- **Consider issues such as ease of use, accessibility, interoperability, and the handling of sensitive information.**
- **Incorporate lessons learned and feedback from previous or similar major events. A needs assessment exercise is a helpful first step to capture the relevant operational requirements and identify gaps in existing procedures and systems.**
- **Understand the resource requirement for each selected solution, in terms of purchase price, operational and maintenance costs, and training requirements.**
- **Estimate the feasibility and potential risk of each relevant solution, especially in terms of end-user acceptance, cybersecurity and data privacy threats, time to implement, and total cost of ownership.**
- **Allow for adjustment and fine-tuning during the trial period and initial implementation.**

24 *Guide on the Security of Major Sporting Events: Promoting Sustainable Security and Legacies*, UNOCT, UNICRI, UNAOC, ICSS, 2021, p. 90.

4.3.1.2 THREATS AND RISK ASSESSMENT

Early in the planning phase, planners must consider eventualities that may expose the community, critical infrastructure, and other soft targets to the possibility of attack during a major event. These activities are categorized as threats and must be assessed in terms of the degree of risk they pose. A comprehensive threat and risk assessment must be made early on for planners to formulate operational plans that mitigate risks.

Conducting a threat and risk assessment involves identifying potential threats such as terrorism, public disorder, criminal acts, harm to image, accidents, emergencies, and disasters (fires, earthquakes, infectious disease, extreme weather events, and more). Any one of these threats can have a catastrophic impact on the event in terms of safety and security. Also, risk assessments need to be conducted of event venues and sites to identify potential areas that are vulnerable to attack. Hence the need to consider threats early on to allow for an adequate planning response. As an example, site risk assessments will be required on stadiums and convention centers and surrounding areas where large crowds or dignitaries will meet to identify areas that may be vulnerable to outside attack.

When assessing threats, one must consider the intent and capability of the perpetrator and the elements of the event itself. Such elements include:

- **Size of the event**
- **Known threats based on similar type events**
- **Significance of the event**
- **Location**
- **Duration**
- **Spectator/participant attendance (cultural, political, or religious backgrounds)**
- **Media coverage**
- **Dignitaries in attendance (heads of state, VIPs who may be targets for attack)**[25]

25 Planning and Managing Security for Major Special Events: Guidelines for Law Enforcement, U.S. Department of Justice.

Risks can seldom be totally eliminated but they can be significantly minimized, contained, or transferred. It is therefore important to develop a risk assessment approach to identify the most significant risks and determine suitable measures to manage them. Risk assessments are based on the likelihood of the threat and the impact it would have on the event should it occur. They are given a numerical rating based on high, medium, or low descriptors. Applying a risk rating to each threat allows planners to provide an adequate plan response relative to the degree of threat. A threat with a high-risk rating would require a more robust planning response than one with a medium or low rating. No threat should be ignored, regardless of its rating, but this type of analysis will help planners consider site vulnerabilities and the appropriate allocation of resources.

Besides being aware of threats and risks in terms of operations, planners also need to consider risks to the planning system itself. The security planning process for a major event can span many years and involve multiple partner organizations. Operational and administrative challenges will require a robust and well-designed planning system. Changes in leadership, operational requirements, funding, human and material resources, logistics and transportation issues, training, and governance all represent risks to the planning process. Mechanisms within the planning system are needed to identify, rate, and mitigate risk, just as in the case of operational threat and risk assessments. For example, human resource allocation is almost always a challenge. The risk assessment mechanism within the planning system serves to mitigate the risk by maximizing the use of technology, using private security, or leveraging the use of human resources between participating agencies.

4.3.2 PILLAR 2: FINANCE

The finance pillar looks at the resources available for the development and implementation of the security plan. Spending for any major international event will be heavily scrutinized by oversight bodies, the media, and taxpayers alike. A robust finance pillar is necessary to ensure that resources are managed effectively and transparently. The lead security agency must secure timely and sufficient funding, first to conduct planning, second to execute the security plan, and lastly to close out the event. Government summits are generally funded entirely by the host government; however, major sporting events usually involve a combination of public and private sector funds, including value-in-kind sponsorship contributions. It will be critical to determine who has specific responsibility for the various security costs and which budget pays for what.

For the publicly funded operations, planners will need to ascertain what will be provided through the regular operating budget of the government department and what will require additional funding sources. One common challenge is that security agencies are asked to submit budgets early in the process, when there are still many logistical unknowns and often before final venue locations and numbers have been determined. The uncertainty is further exacerbated by inevitable ongoing changes to planning assumptions and pending or delayed procurement decisions, which often increase costs. Therefore, it is critical to factor in contingencies to address changes to the original budget assumptions.

In addition to the costs involved in protecting the event venues themselves, there will also be costs to enhance security around critical infrastructure (such as electricity/water/transportation networks) and potential soft targets near the event (crowded parks, community events, bars). These costs should be negotiated, clarified, and determined as early as possible.

Security costs for a major event can be considerable, but so can the benefits. At a time when the spotlight of the world is on the host country, the investments made in a robust security system will leave a lasting positive legacy.

4.3.2.1 BUDGET

Security budgets for major events will differ widely depending on the nature of the event and such factors as the size, location, duration, and specific threats and concerns. However, it is safe to say that the cost to secure any major international event is likely to be enormous, running into the tens and even hundreds of millions of dollars. No host country has an unlimited budget, so planners will need to find additional sources of funding and wisely manage the resources available.

Ineffective budgeting will obviously hurt the planning process. Sound financial management practices are required to define security costs and benefits more precisely. It may be useful to apply several approaches, such as modeling budgets, using benchmarks from similar past events, conducting a risk analysis of security costs, and applying options and cost-benefit analyses.[26] Individuals responsible for the financial management of such a large budget must be properly qualified and experienced and must have financial approval authority.

The main security costs for most events include:

- **Personnel and overtime (large planning team for months or years and major operational deployment)**
- **Temporary accommodations for workforce (often with elevated hotel costs at event time)**
- **Contingency planning**
- **Perimeter intrusion detection system**
- **Fencing**
- **Radio telecommunications**
- **Security workforce travel to/from the event location**
- **Leased office space for planning (years)/ warehousing (in the lead-up to and after the event)**

26 IPO Security Planning Model, International Permanent Observatory on Security during Major Events, United Nations Interregional Crime and Justice Research Institute (UNICRI), 2007.

4.3.2.2 COMPENSATION

Salary costs and overtime will often be substantial. In most cases, out-of-town police agencies that contribute law enforcement resources will expect to fully recover any costs they incur. In some cases, this will include the staffing costs involved at the home location to fill in for the officers who have been seconded to the event. If the event will take place a few years after the initial budget exercise, projected salary increases and inflation should be taken into account. Consideration should also be given to the costs of employee benefit packages for the long-term planning staff.

4.3.2.3 CONTRACTING AUTHORITIES

The purchase or lease of many of the large-scale items and services mentioned in this document will require exceptional financial authority for contracts and purchase orders. Many of these items will require sufficient lead time for delivery, so it is imperative that the procurement officers have the appropriate spending authority and approval processes in place to ensure that all legal requirements are met. An example of a large-scale contracting requirement is the matter of local accommodations for law enforcement officials who come in from other areas. Tens of thousands of room nights could be needed for a long-term event like an Olympic Games or FIFA World Cup. Contracts to secure sufficient rooms are expensive and will require special signing authority. Similarly, private security costs can be massive, especially when costs for recruitment, training, uniforms, equipment, accommodations, and transportation are factored into the budget. Complicating the matter, funding sources may involve several levels of government with varying protocols and processes. All this needs to be mapped out at the onset of planning.

4.3.2.4 AUDIT AND EVALUATION

The work of the finance pillar will also include evaluating the benefits and suitability of assets (value for dollar) for similar types of events in the future. The evaluation is of benefit for the security planners, who will be required to give an accounting to the government, as well as for donors and sponsors that have provided funding or material assets to support certain security planning requirements. Some questions that will be asked in the evaluation are:

- **How did the costs benchmark against similar events in the past?**
- **Were salary and overtime expenses managed efficiently and effectively?**
- **What processes and mechanisms were in place to control spending?**

Government oversight will be particularly interested in the impact on taxpayers. Scrutiny will be placed on items normally bought during regular law enforcement business, such as radios, weapons, and laptops. If an actual audit is requested, auditors will want to ensure that expenses and disbursements were reported accurately and in a timely manner.

4.3.3 PILLAR 3: LEGAL

During the planning phase, activities that involve multiple partners and stakeholders will require numerous contractual agreements. The legal pillar must ensure compliance with all obligations generated by the different sources, ranging from international governments to private companies. Additionally, legal services should be deployed to represent the various stakeholders involved in any dispute that may arise in connection with the security planning of the event. Any liability issues stemming from the use of human and material resources, cost-sharing agreements, or other matters must be addressed.

Legal professionals will need to be involved in every stage of the event, from planning to close-out, to provide guidance on all legal issues and challenges. During the implementation of the security plans, organizers may need to obtain court orders to prohibit unauthorized access to event venues or respond to lawsuits filed on behalf of protestors seeking to limit security measures. Those responsible for the execution of security functions must follow the legal parameters set by domestic laws and by international standards, 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.

More broadly, all security activities must respect national norms and laws, as well as international human rights standards regarding freedom of speech and expression, freedom of assembly, the right to humane treatment, the right to privacy, and all other fundamental rights and freedoms.

4.3.4 PILLAR 4: SAFETY AND SECURITY

Security planning is all about ensuring a safe and secure environment for event participants, VIPs, official dignitaries, and the general public. With that in mind, the safety and security pillar has the responsibility to produce the core output of the process, the operations plans. This is the largest and most complex pillar under this planning model.

Operations plans are produced in consideration of the event program and based on a comprehensive threat and risk assessment. They focus on several key areas: land operations, air operations, marine operations (where applicable), and cybersecurity operations. The task here is broad:

- **To provide an effective intelligence-led response at the earliest opportunity;**
- **To detect and try to prevent the entry of individuals seeking to disrupt the event in any way;**
- **To detect and try to prevent a range of event-related illegal activities; and**
- **To enhance information sharing.**

Given the centrality of operations plans, careful record-keeping and reporting will be a core responsibility for this pillar. It will allow support planners to provide the resources needed for execution and allow procurement planners to receive those resources within the required time frame. This will provide for better forecasting of resource requirements and financial projections during the planning phase.

As with all the work areas, the safety and security pillar must have the capacity to manage all these requirements. The priority is to identify the functional needs of each pillar and acquire the necessary human and material resources it needs to complete its tasks and interact with the other pillars. For more details about the different elements of the operations plans, see Chapter 5.

4.3.5 PILLAR 5: LOGISTICS

Logistical support is critical to the successful execution of security planning, management of assets, and procurement of material and human resources throughout all phases of a major event. The logistics pillar, which is responsible for producing and implementing support plans, must begin its work early on in the process and coordinate closely with security planners and finance managers. Ongoing assessments of security needs as they unfold will avoid duplication of assets and human resources. The logistics team will have to assess the logistical requirements of the entire security planning system to ensure that each work pillar has access to the resources it needs to function. The likelihood is strong that demand for logistics resources will exceed the national supply in several areas, so it will no doubt be necessary to apply mitigation strategies such as leveraging additional support from other sources or making more effective use of technology.

The work of the logistics pillar typically comprises two branches: logistics support and logistics procurement. See Chapter 5 for more details.

4.3.6 PILLAR 6: COMMUNICATION

A strong communication strategy related to security is critical to the success of every major event. The communication pillar will look at both internal and external communication, including social media networking sites, media relations, and community relations. It should develop an integrated strategy involving all security stakeholders from the government, the organizing committee, and outside partners, using a centralized messaging model. This can be accomplished through the creation of an integrated security communication team (ISCT) which engages in ongoing outreach to all stakeholders. This allows the team to dismiss rumors early, build a good reputation, answer questions, and gather intelligence. Among the objectives: to build and maintain public confidence in the security measures; to engage in transparent and timely interactions with the media and other external stakeholders, while protecting the integrity of the security operations; and to provide clear, timely communication with internal and external audiences. The mandate of an ISCT is to share information and address communication and media issues that may affect the security of the major event.[27]

It is also important to create internal and external crisis communication plans which will enable organizers to anticipate emergency situations by having clear, consistent messaging and appropriate protocols at the ready, including pre-existing dissemination networks. This will help to minimize or mitigate the situational impact and risk.

Ideally, the ISCT will be embedded with the overall command-and-control framework during the event, in order to react in real time to any fast-moving situation requiring a coordinated communication response.

Chapter 5 breaks down the different elements of internal and external communications, but in general terms, a strong communication strategy is intended to:

- **Create a positive image for the event;**
- **Keep the public appropriately informed through the media;**
- **Provide regular updates of aspects that will directly affect people's lives, such as traffic disruptions, recommended routes, ticketing arrangements, and event venues;**
- **Monitor international, national, and local media coverage;**
- **Develop strategies to ensure fair and accurate reporting;**
- **Designate spokespersons and develop policies and procedures for managing all official responses to media comments on security; and**
- **Coordinate and facilitate press conferences on security.**

27 *Guide on the Security of Major Sporting Events: Promoting Sustainable Security and Legacies*, UNOCT, UNICRI, UNAOC, ICSS, 2021, Chapter VIII

4.4 THE PLANNING EXECUTION

4.4.1 SYSTEMS BUILDING

It is important to understand how systems work. The SIPOC model organizes systems into its basic components: sources, inputs, processes, outputs, and customers. Systems building encapsulates the project strategies, tactics, policies, procedures, and rules that drive the functional process to deliver outputs. Understanding and adhering to these activities is especially useful when multiple agencies are working toward a common objective.

Strong leadership, good governance, stakeholder engagement, communication, and timely and accurate intelligence must all work together to support a security planning system that takes inputs, processes them, and produces outputs to meet the strategic objectives. For this type of multi-agency organization to operate in a changing environment, the planning system will have to meet several key requirements.

- **It should be capable of producing the plans required to meet the project mission. Are the system components efficient in terms of scope of work, given the available time?**
- **It should have the human and material resources needed to process large volumes of work within critical time frames.**
- **It should be able to overcome unexpected challenges that require a quick response. Venue changes, human resourcing shortfalls, technology failures, disagreements over areas of responsibility, public health issues, and extreme weather conditions are just a few examples that must be overcome.**[28]

4.4.2 THE INTEGRATION MECHANISM

As mentioned at the beginning of this manual, security planning is not an exercise to be done in isolation. Rather, it must be developed within the specific framework and under the specific circumstances applicable to the hosting country at any given moment. In addition, some of these circumstances may change during the different phases of the planning, up to the time of implementation. For this reason, security planning is a living exercise, one that must be able to nimbly absorb and respond to surrounding circumstances and emerging issues.

To reflect the particular circumstances involved, the host country has to shape the design and implementation of the security planning process and ensure that it can adapt to change. According to the *Guide on the Security of Major Sporting Events:*

28 *Guide on the Security of Major Sporting Events: Promoting Sustainable Security and Legacies*, UNOCT, UNICRI, UNAOC, ICSS, 2021, Chapter VII.

> Government oversight, political policies, financial constraints, and the ability to mobilize human and material resources within the required time frames have an impact in the planning and delivery of security. That is why systems must have the capacity to adapt to challenges.[29]

To take into account the complexity of evolving circumstances which may affect all the agencies involved, at both the strategic and operational level, the decision management mechanism must be designed to integrate all the relevant stakeholders. This gives them the chance to adapt their course of action as necessary and also frames their contribution to the security plan.

For example, if an unexpected crisis unrelated to the security plan requires the increased attention of one particular agency, that agency will need to communicate with the lead security agency and explain how and to what extent the crisis will affect its capacity to support the event as originally envisaged. The lead security agency, for its part, must evaluate the implications, determine what inputs may be lacking from the agency in question, and then redistribute tasks so as not to affect the final outputs (namely, the various plans outlined in Chapter 5).

The diagram that follows represents a proven integrated security planning system that has been used and validated in the context of major events.

29 Ibid., p. 105.

Integrated Planning Scheme

Diagram 5[30]

Note: JOPG stands for joint operational planning group.

30 Source: Brian London, Superintendent (Retired) Royal Canadian Mounted Police. Lead Planner, 2010 G8 and G20 Summits. Developed in the context of the Guide on the Security of Major Sporting Events: Promoting Sustainable Security and Legacies, UNOCT, UNICRI, UNAOC, ICSS, 2021

- **In the above diagram, the senior executive team (at the political/strategic level) sits above the overall mission, reflecting its strategic position in the event hierarchy. It does not direct the security planning process but is responsible for high-level strategic decisions which may affect the security plan.**

- **The strategic direction component brings in specific considerations with the goal of achieving the long-term strategic or critical objectives of the security plan.**

- **Integrated planning provides the lead security agency's senior management team with a broad overview of the security requirements and partner capabilities at the strategic level, beyond the security plan itself. The senior management team is responsible for designing and implementing the security plan and ensuring the strategic objectives are on track. It assesses risk tolerance and guides solutions to problems and challenges encountered by the various entities that work within the security planning system.**

- **At the operational level, all the different entities and agencies involved in the security plan are organized into a joint operational planning group (JOPG), which plays a tactical role and takes any short-term steps and actions required to achieve the objectives of the strategic plan. The JOPG is composed of mid-level managers representing all the stakeholders involved, enabling them to engage in open and collaborative communication. The mechanism incorporates each agency's perspective while implementing practical operations, within the broader framework of interagency cooperation and public-private partnerships established at the strategic level.**

Within the JOPG, two types of operational groups should be established to continually update the senior management team on any evolving circumstances that should be taken into consideration at any time throughout the different planning phases.

- **The integrated risk management group is designed to assess emerging threats and mitigate related risks. To ensure situational awareness, this group provides the senior management team with information/intelligence (inputs) from the perspective of the different agencies (sources) involved in the planning.**

- **The issue management group, for its part, keeps the senior management team informed about potential issues that may arise and need to be resolved, such as funding, program changes, and logistical concerns. This group reports on possible changes in resources and obligations (inputs) from the perspective of the different agencies (sources) involved in the planning. Issue management groups are made up of JOPG members and tasked with making recommendations in response to specific problems that arise during planning.**

Such mechanisms for interaction between the senior management team and the joint operational planning group are essential to initially shape and then continuously adjust the planning process in light of changing circumstances. That will lead to the most efficient use of the inputs in the implementation of the outputs (the various security plans explained in Chapter 5).

4.4.3 THE PLANNING ASSUMPTION PROCESS

At the start of the planning process for a major event, the organizational committee takes the first steps toward formulating a tentative event program, which will evolve into its fixed and final state throughout the planning phase. The initial risk for planners is that they must project the requirements for human resources, goods and services, and assets based on uncertain information. Finance, in turn, must make initial budget assessments based on this same information. Planning has to proceed based on program assumptions, and planners should track all changes as the event becomes more clearly defined, as explained below. While this process can be challenging, the effort will prove its value after the event, when planners must account for the money spent and any cost overruns. The list of changes and any supporting documentation should be included with budget forecasts. Tracking these issues from the beginning will help security planners defend their requests for additional resources should the project scope change substantially later in the planning phase.

4.4.4 THE OPTIONS ANALYSIS AND THE CHANGE CONTROL PROCESS

While the logistics pillar is responsible for the acquisition of material resources, it is the project management's responsibility to ensure that proper protocols are followed so that the best and most cost-effective solution is identified to address the specific need. Management must also ensure that those responsible for procurement do an options analysis before acquiring goods and services or material assets.

During the plan validation process, planners can expect to identify many weak links and gaps that will need to be changed. There must be a formal management process to track and coordinate those changes. For example, changes to staffing levels have a cascading impact on planning for transportation, accommodations, and meals; this in turn affects the financial aspect. This process continues throughout the planning phase. As the clock ticks down to the event, plan managers need to continuously identify all relevant changes and report them to a change control coordinator. That person will use data management software to determine the impacts of the changes on costs and resource requirements and will keep the relevant work pillars apprised so that they can revise their specific plans accordingly.

4.4.5 INTERDEPENDENT AND INTEROPERABLE PLANS

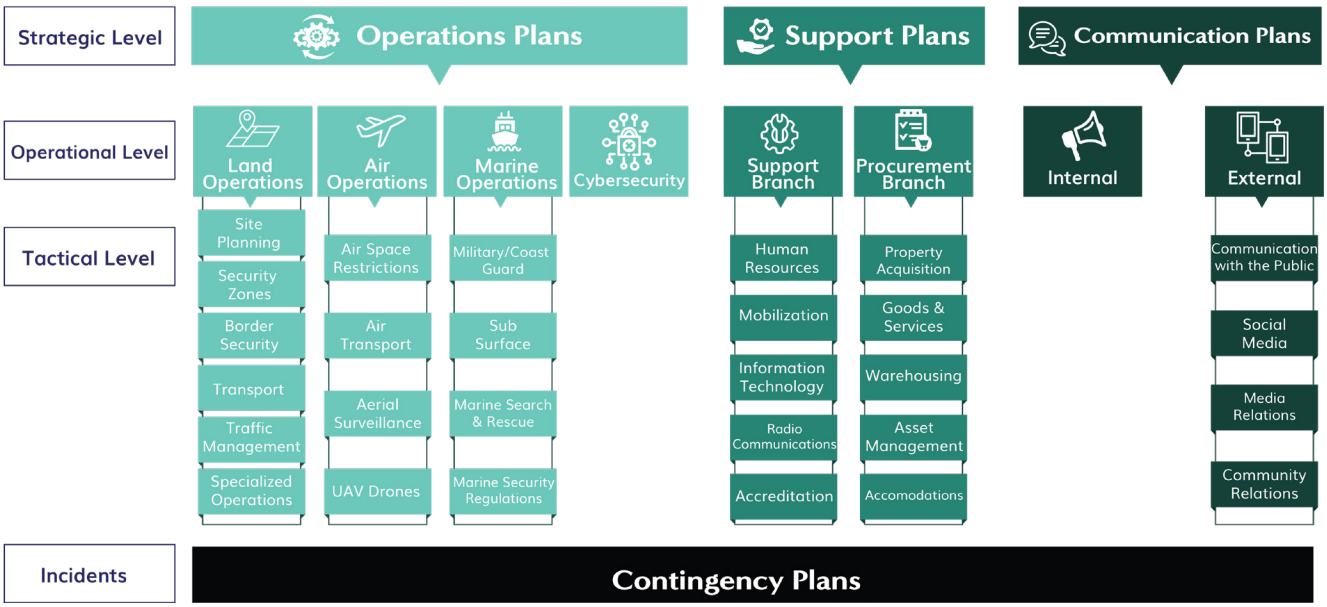
The organizational planning structure must promote an integrated approach to planning, recognizing the interdependent relationships between all the work pillars and with the security partners. This will ensure that the plans produced are interoperable, meaning they are synchronized to work together during the operations phase regardless of jurisdiction, policy variances, information management technology systems, human resources, and other factors. In the absence of an integrated approach, commanders might unexpectedly encounter significant operational gaps when the plans are executed.

Transportation, for example, is a critical component of any major event, covering not only the movement of VIPs but also the logistics of getting members of the security workforce to their posts on time and enabling guests, spectators, and the public at large to reach their destinations safely. A robust transportation plan is required to interact with other event plans related to venue access. Transportation planners need to understand work schedules, the number of staff to be moved, the location of accommodation sites, and the anticipated impact on the general public in order to determine busing routes and departure schedules. Long before the event, they need to advise procurement planners on vehicle requirements, to allow sufficient time to prepare contracts and ensure timely delivery. Finance will also need to know the projected costs to manage the budget. Eventually, the communication team will need detailed information so that it can advise its internal and external audiences about special busing routes and possible road closures or traffic congestion.

As is evident from this example, transportation is so closely interconnected to other areas—including accommodations, procurement, finance, and communication—that any plan that did not factor in this interdependence would be inoperable.

This kind of synchronized planning relies on a collaborative planning structure. Management and the lead security agency must build a planning organization that fosters collaboration and integration between the pillars and all security partners.

CHAPTER 5: OUTPUTS



Outputs are the end products that emerge from the security planning process—in this case, an interdependent set of plans—thanks to the efforts carried out through each of the work pillars. The three main categories of plans cover operations, support, and communication; these are supplemented by contingency plans. In general, the plans are designed to:

- **Save lives, protect property, and prevent crime inside the designated secure areas;**
- **Save lives, protect property, and prevent crime outside the designated secure areas;**
- **Ensure coordination, enhance public confidence, and minimize potential damage to reputation; and**
- **Provide a contingency response should there be a critical event.**

5.1 OPERATIONS PLANS

Operations plans focus on securing all aspects of the major event, such as site and venue security, motorcade movements, cybersecurity, VIP protection, transportation, and much more. These plans are formulated by the safety and security work pillar. They are broad in scope, covering air, land, and marine components, and can be scaled up as needed. They include deterrence and intervention measures intended to prevent malicious acts meant to cause severe harm or injury to people or destruction of property. The section below looks at some of the considerations that will go into these operations plans.

5.1.1 LAND OPERATIONS

Land operations are designed to prevent, detect, deter, and interdict anyone trying to infiltrate the security footprint by land. They provide multi-layered secure zones by employing coordinated tactics that ensure the safe and effective movement of event participants and the public. One example is the use of physical infrastructure, such as perimeter security fencing, to surround event sites. Because this type of security often requires large deployments of personnel and major infrastructure resources, the unique capabilities of military personnel and resources are often used to support police operations. Private security may also play a significant complementary role.

5.1.1.1 SITE PLANNING - EVENT/ NON-EVENT SECURITY

The aim of site planning is to anticipate and interrupt problems and threats before they reach anyone inside the event area—including participants, spectators, and security and non-security staff—but also to consider the risk to the general public outside the security perimeter.

Site and venue security planning involves identifying and securing areas within and around event sites. Every site will need to undergo a vulnerability risk assessment to identify areas vulnerable to attack, followed by the formulation of remedies to lower the risk and secure the area. Once the site is hardened and secured, an accreditation system will be needed to prevent access by unauthorized people. Contingency plans will have to be developed to designate site access and egress points for participants, delegates, or spectators in the event of an attack or an unsafe situation. Event sites include hotels where participants and staff are staying, sponsor villages, media centers, or places designated for related activities, such as fan parks or designated protest areas.

Planners should also consider extending the security footprint outward from the secure zone to non-event sites. The aim here is to intercept problems before they reach the secure area. Depending on the police force of jurisdiction, planners may also want to include measures to prevent crime and protect people and property in places such as shopping centers, tourist attractions, and historical monuments.

Non-event sites include facilities that the host country considers "critical" infrastructure for purposes of national security. Critical infrastructure may include nuclear and chemical industry installations, gas and oil pipelines, electric power substations, waterways, major transportation links, and communication infrastructure such as cell towers.

A visual representation of the security zones is referenced below.

5.1.1.2 SECURITY ZONES

Ground-based security operations are managed in accordance with the layered security concept depicted in the diagram below. Site planning uses an internationally accepted practice which secures a site from the center and works outward in concentric or eccentric circles, each circle representing a different level of security. These circles are known as security zones. The innermost secure area is the controlled access zone, the next outward ring is the interdiction zone, and the third is the surveillance zone.

Diagram 6

Controlled access zone (CAZ)

This area, sometimes called the inner security perimeter, usually falls under the responsibility of the lead security agency. The primary tasks are to secure the controlled access zone and prevent destruction or loss, and to remove all threats from the zone through physical verification. This area is characterized by:

- **Accredited access (delegates, media, designated security personnel)**
- **Comprehensive vehicle inspections (visual, canine, X-ray, explosive detection unit)**
- **Perimeter integrity (physical barriers, electronic surveillance, security forces)**
- **Vehicle/vessel exclusion**

Interdiction zone (IZ)

This area, which may also be referred to as the outer perimeter, usually falls under the responsibility of the police force of jurisdiction and involves sealing off or controlling the use of a route or approach. It is characterized by:

- **Accredited access (residents)**
- **Vehicle inspection (accredited, visual)**
- **Perimeter integrity (physical barriers, electronic surveillance, security forces)**
- **Vehicle/vessel exclusion**

Surveillance zone (SZ)

This zone extends outward from the interdiction zone and is a shared responsibility of all event partners, including security agencies, the general public, and organizing bodies. The primary task here is screening, in other words, observing, identifying, and reporting information. Tools include:

- **Police patrols (vehicle/vessel/aircraft/foot)**
- **Checkpoints**
- **Surveillance**

5.1.1.3 BORDER SECURITY

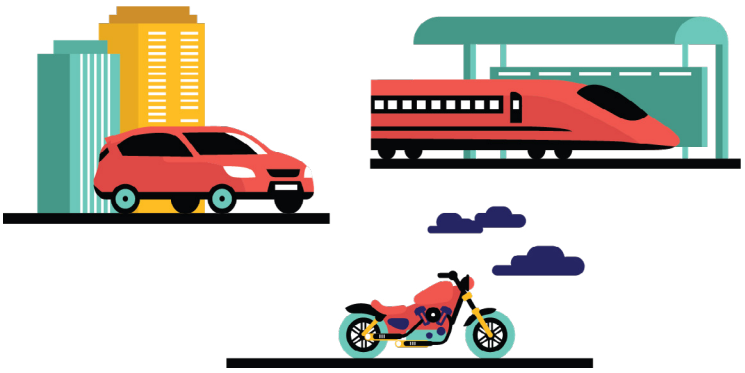
Security planners for major events must also ensure a direct link between their operations plan and the national border services and immigration authorities, as the *Guide on the Security of Major Sporting Events* explains.

> Ensuring effective border security is an integral part of any comprehensive and integrated national counter-terrorism strategy and requires collective action by States and relevant international and regional organizations. For example, Coordinated Border Management (CBM) strategies, which require close coordination among the competent authorities at border locations, have in many cases proven to be a highly effective tool for managing national borders.[31]

Based on the analysis of intelligence information and the assessment of specific risks, the host country may decide to designate a period in which to establish special border control activities. This would:

- **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; and**
- **Provide opportunities to enhance information sharing and the collection of event-related information and intelligence.**[32]

5.1.1.4 TRANSPORT



In the context of operations security for a major event, transportation planning encompasses the measures needed to safely transport VIPs, dignitaries, and participants, be it by land, air, or water. It also covers the movement of security personnel and assets between different sites (work, accommodations, meals).

31 *Guide on the Security of Major Sporting Events: Promoting Sustainable Security and Legacies*, pp. 114-115.
32 IPO Security Planning Model, p. 13.

5.1.1.5 TRAFFIC MANAGEMENT

A traffic management plan involves working with civilian transportation authorities to secure access routes to and from venues and other event sites for the event participants. A primary priority is to prevent traffic congestion that could lead to accidents or provide terrorists a focal point to carry out an attack on motorcades or on the general public.

One task will be managing road closures and maintaining a secure and viable road network not only within the event footprint but beyond. This may involve suspending roadworks, securing bridges and tunnels, reviewing speed limits, and implementing other forms of traffic control. It is also important to prepare contingency plans to deal with traffic disruptions or the blockage of routes by accidents, protesters, or any other incident.

5.1.1.6 SPECIALIZED OPERATIONS

Every major event will require specialized law enforcement services to be deployed in one or more of the designated domains for land, air, or marine operations. The unique demands of each event will dictate which specialized units will be required, although planners should anticipate that most of these units will be deployed or should at the very least be readily available.

Specialized units offer niche capabilities and a surge capacity. They can be deployed to sites to provide a deterrent presence or respond to incidents within the event area of responsibility. Specialized units include, but are not limited to, the following:

- **Canine units – Law enforcement service dogs are used extensively for explosive detection during security sweeps and at venues such as airports and marine ports of entry. Specially trained dogs can also be used for search and rescue, crowd control, and drug detection.**
- **Mounted units – Horses can provide additional support for crowd control or patrols in urban and rural areas.**
- **Bicycle units – Patrol officers on bicycles can maneuver well through congested traffic or confined areas, and position themselves to assist with crowd management.**
- **Motorcycle units – These are often used to control traffic and escort motorcades.**
- **Rapid response teams – Mobile patrol units are able to supplement foot patrols and static posts as needed.**
- **Emergency response teams – These are law enforcement tactical teams (SWAT units) trained to handle particularly dangerous situations.**
- **Explosive detection disposal units**
- **Hostage negotiators**
- **Public order units – These units handle crowd management or riot control.**
- **Forensic identification units – In the event of a crime, such units would investigate the crime scene and gather evidence.**
- **Obstruction removal teams – They would dismantle any barriers or remove objects set up to disrupt movement.**

5.1.2 AIR OPERATIONS

The purpose of air operations is to employ integrated aviation safety planning to prohibit unauthorized aircraft from entering the airspace over the event. This integrated approach involves a multilayered air safety net for the event which would include: the development and enforcement of notices to air missions (NOTAMS), which communicate essential information about flight operations; the monitoring and control of airspace in the vicinity of airports; the development and exercise of air rules of engagement in an integrated manner to the highest levels; and the utilization of the unique capability and assets of military and other agency aerial resources. The safety and security pillar should create a specific air operations cell to address such issues.

5.1.2.1 AIRSPACE RESTRICTIONS

Authorities will often designate a restricted airspace in connection with a major event, to enable safe management of air traffic associated with the event and to help ensure that unauthorized, non-participating aircraft will remain clear of the airspace surrounding sensitive activities. Restricted airspace activation should coincide with the arrival and departure dates of the visiting government dignitaries or event-specific activities.

Depending on the type of major event and when appropriate, the safety and security pillar's air operations cell may want to establish an integrated airspace authorizations unit to manage requests from aircraft operators wishing to enter restricted airspace. Pilots should read all applicable NOTAMS and contact their local flight service station prior to flight operations. It is the pilot's responsibility to ensure that proper authorization has been obtained prior to starting flight operations.

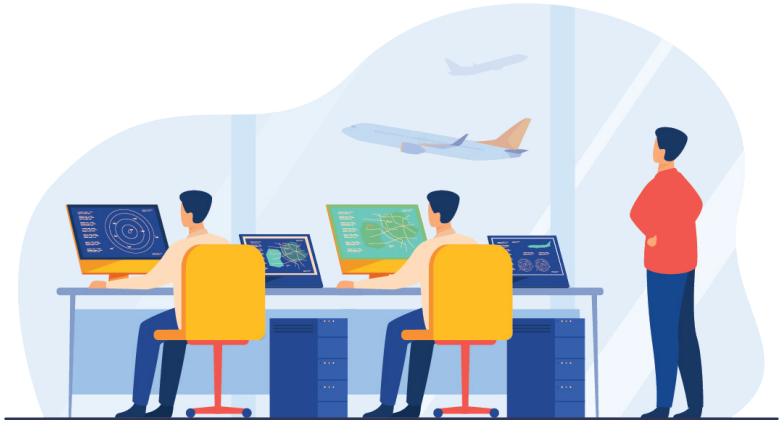
Sporting event waivers can permit flight operations within the temporary flight restricted airspace for approved media aircraft. Such waivers are event-specific. Each approved waiver will specify the name, dates, and location of the specific sporting venue over which the pilot will be authorized to fly.

National aviation regulations describe special flight rules areas and flight restricted zones; such regulations are supplemented as necessary by NOTAMs and published in compliance with regulations established by the International Civil Aviation Organization (ICAO).

Varying swaths of airspace may be subject to flight restrictions to accommodate the event. Some restrictions will be in place days or weeks before a major event, especially for political summits. The restrictions can be complex and overlapping in nature and may affect multiple airports, seaplane bases, and heliports.

During specific time frames, access will be limited to approved military or police operations and emergency/lifesaving flights (including MEDEVAC flights), search and rescue, approved essential-service aircraft, state aircraft on official business, and aircraft carrying police-designated VIPs or internationally protected persons such as diplomats or heads of state.

Operators and/or flight crews will be required to submit a flight authorization request for each flight. All flights into a restricted airspace must be authorized by the proper authorities on an individual-mission basis. Errant aircraft may be intercepted by military or law enforcement aircraft.



5.1.2.2 AIR TRANSPORT

The air operations cell will not only handle the security aspect but also ensure that specific air assets are available for tactical transport activities. With thousands of security personnel moving into and out of the event operational theater, commercial or government aircraft may be needed to transport them to and from their home bases or collection points. Similarly, during the event operations, aircraft may be needed to transport security personnel, equipment, or VIPs between geographically dispersed venues. Aircraft must also be available to move specialized units, such as SWAT or medevac teams, on an urgent basis. Plans must be interoperable to ensure that assets can be moved safely and efficiently before, during, and after the event, within the constraints of any airspace restrictions.

5.1.2.3 AERIAL SURVEILLANCE

In order to secure the airspace, there must be a process in place to control and monitor all aircraft flying in and around the event operational theater and to respond to any airborne threat. As was seen during the September 11, 2001, attacks in the United States, aircraft themselves can be weaponized to effect significant death and destruction. Aerial surveillance capabilities are required for both airborne and ground- and water-based detection and observation. When appropriate, planning for a major event should include military assistance for radar and geospatial capabilities, as well as additional aerial surveillance technologies such as aerostats, robots, drones, and tethered balloons.

Aerial surveillance aircraft and other assets can aid in monitoring large-scale areas and can be equipped with technology that can livestream video from the aircraft to personnel on the ground. By improving connectivity and communication, it can also strengthen collaboration among security personnel.

5.1.2.4 UNMANNED AERIAL VEHICLE (UAV) – UNMANNED AIRCRAFT SYSTEM (UAS) – DRONES

In recent years, drone technology has become much more prevalent during major events, used for TV broadcasting, officiating, and advertising, among other activities. The use of drone and counter-drone technology is now a fundamental operational component of event security as well. Proactively, UAV and UAS technologies can offer a higher-altitude surveillance, tracking, and monitoring capability; reactively, they provide another means for detection and interdiction.

Counter-drone technology—also known as counter-UAS, C-UAS, or counter-UAV technology— refers to systems used to detect or intercept unmanned aircraft. UAVs are considered a top threat posed by terrorists, criminals, or just spectators looking to circumvent the normal fan experience.

Detection tools include radar, radio frequency, electro-optical, infrared, acoustic, and combined sensors capabilities. Interdiction tools include lasers, entanglement nets, radio frequency jamming, electromagnetic pulse, "suicide" drones, and various combinations of these tools and others. C-UAV/UAS systems can be ground- or air-based or even handheld. The rapid development of new platforms makes it difficult to be fully up-to-date, so this element of the planning/operations team must include expert practitioners who know the latest technology and can create an effective operational response.

5.1.3 MARINE OPERATIONS

The task of the marine operations cell is to ensure effective protection of all event sites near the water. It conducts vulnerability assessments of all marine sites; strategically deploys marine assets; integrates marine assets with land and air security elements; identifies marine exclusion zones and communicates the information to the general public and key stakeholders; and ensures that the unique capabilities and assets of the military and coast guard work in sync with police marine units to ensure that water-based operations compliment integrated land operations.

5.1.3.1 MILITARY/COAST GUARD

For events held near large bodies of water or major marine navigational routes, the integrated security planning team should include planners from all relevant national agencies, such as the Coast Guard, the Department of Defense (Navy), Customs and Border Protection, and the government department responsible for maritime transportation regulations. These agencies can provide the capacity to deal with marine incidents requiring larger or more specialized vessels.

5.1.3.2 SUBSURFACE

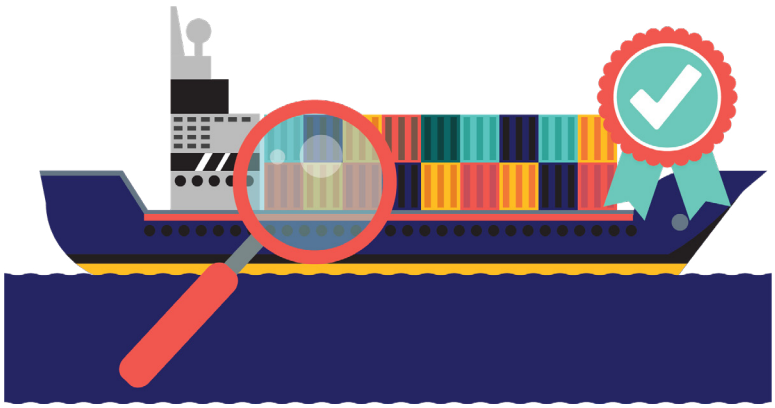
Subsurface security is another area that warrants attention. Planners may want to consider using underwater sensors capable of detecting subsurface threats. In advance of the event, divers and underwater surveillance equipment should be used to conduct security sweeps and periodic inspections of vessels and subsurface infrastructure. Furthermore, law enforcement explosive detection units or ordnance-qualified naval divers should be at the ready to respond to any reported or actual threat of an underwater or vessel-related explosive device. If the capability exists for underwater imaging, this should be employed at regular intervals prior to and during the event, and the images should be collected and analyzed for anomalies.

5.1.3.3 MARINE SEARCH AND RESCUE

This aspect of marine operations refers to the capability to search for or provide assistance to persons, ships, or other craft that are, or are feared to be, in distress or imminent danger. Search and rescue capability should be available if the event locations are near large bodies of water. Despite lawful exclusion zones and restrictions, boaters or protesters sometimes try to breach the security perimeter by water and can find themselves lost or in distress as a result. Search and rescue units may be required to render assistance.

5.1.3.4 MARINE SECURITY REGULATIONS

Host nations will likely have laws or regulations in place related to maritime transportation security, based on guidelines developed by the United Nations International Maritime Organization. These national legislative provisions can normally be used to establish lawful marine exclusion zones on waterways surrounding the event location. In cases where no legal authority exists, it may be necessary to initiate regulatory reform well before the event so that the mechanisms to establish enforceable exclusion zones are available.



Marine security operations bulletins provide guidance on specific situations. The bulletins cover matters such as the implementation of marine security legislation, rules and regulations for industry facilities operating in the area, enforcement of compliance, or marine security documents. They are developed and issued to ensure effective cooperation and coordination among all stakeholders involved, thus enhancing the marine security posture around the event.

5.1.4 CYBERSECURITY

Event organizers rely heavily on technology, which intensifies the need to protect data and networks from a variety of cyberthreats, whether from state or non-state actors. A broad cyber defense strategy is needed to guard against malicious acts such as denial-of-service attacks, in which hackers attempt to disrupt the normal traffic of a targeted server. The cybersecurity defense plan put together for a major event should complement and make maximum use of existing national cybersecurity agency structures and international partnerships against cybercrime. The major event's cybersecurity team should include trusted government and private sector security specialists in information management and information technology, as well as law enforcement investigators. Together, they need to develop and implement a comprehensive plan to deal with cyberattacks, based on "detect, respond, and recover" capabilities. Such a plan should include a defense mechanism for computers, servers, mobile devices, electronic systems, and other network components.[33]

Cyberattacks can be external or internal. In the former case, external actors may hack into a network to steal or manipulate data as a way to disrupt the event or cause negative publicity. Alternatively, an attack can originate from the inside, such as from a disgruntled employee who may have the motivation and capabilities to compromise data. Experience has shown that internal bad actors are especially dangerous because of their access to the event's networks and information systems. With this in mind, it is important to implement prudent screening procedures and background checks when selecting the entire planning team and to ensure that employees are appropriately compensated, commensurate with their respective duties. Both internal and external threat sources must be taken seriously.

33 *Guide on the Security of Major Sporting Events: Promoting Sustainable Security and Legacies*, p. 111.

5.2 SUPPORT PLANS

Just as the name implies, support plans are designed to provide the appropriate logistics and resource support needed to execute the operations plans. Support plans may include, but are not limited to, private security, accommodations, logistics, mobilization of human resources, knowledge transfer, and information technology. It is the logistics work pillar identified in this planning model that is responsible for formulating these plans.

5.2.1 THE SUPPORT BRANCH

The logistics support branch oversees such things as the movement of security personnel and material assets required throughout the security footprint. This will require a transportation plan; for example, a fleet of buses may be needed to move personnel, while trucks and vans may be required to transport assets. This information will have to be made known to the procurement team. Logistics support also evaluates the human resources and job skills required to fill certain functions and the eventual mobilization of those resources, first for planning and later to implement the operations plans. Other critically important areas include information technology, radio communications, and accreditation requirements.

5.2.1.1 HUMAN RESOURCES[34]

The scale of planning for a major event almost always goes far beyond what was initially envisaged. It is easy to underestimate the complexity of establishing the human, physical, and technological resources required to execute the plans. In fact, a major international event may well come close to exhausting the national resources available in some aspects of operational activity, physical security infrastructure, and transport requirements.

It is therefore for planners to determine and select the correct number of trained, qualified, and properly equipped staff across the range of security skills and disciplines.

The staff-related challenges that planners will have to solve are multiple and often mundane: workable shift rotations, toilets for staff, shelters for their service dogs and horses, prevention of food poisoning, charging stations for thousands of mobile devices, secure storage of firearms, even the availability of insect repellent.

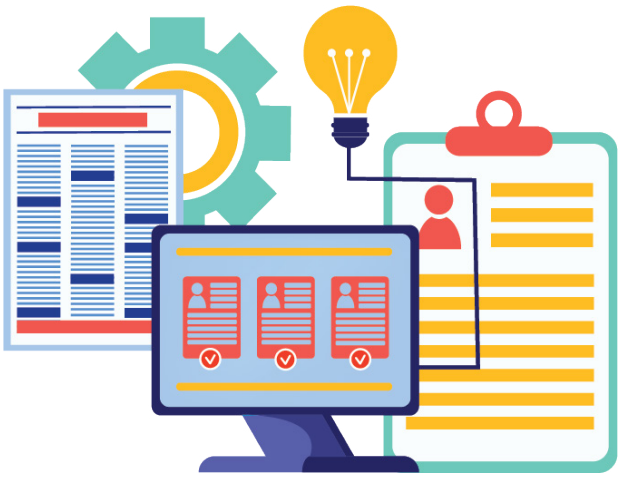
And the need for sufficient resources for event security must be weighed against the reality that the host location will still need law enforcement outside the event venues. Because of the strain on the availability of staff and equipment, the security planning team must coordinate closely with local law enforcement to achieve the best possible use of resources.

34 See also Chapter 3.2.1 of this manual.

5.2.1.2 MOBILIZATION OF HUMAN RESOURCES

One of the most complicated and stressful tasks of planning a major event is the need to mobilize human resources—in other words, to muster the people needed to meet operational requirements in specific places at specific times. Mobilization planners need to be in constant contact with every pillar of the operation to identify human resource needs, both in the planning phase and during the larger-scale security operations. There are strong interfaces between mobilization, transportation, accommodations, and meals.

A poorly planned and poorly coordinated mobilization process will have lasting negative impacts on both the perception and the quality of event security. Experience has shown that the workforce needs to have comfortable accommodations and quality food and be adequately compensated for the work performed.



Because of the complexities involved, a dedicated group should be created early on to take charge of this function, with clearly defined roles and responsibilities. The mobilization role includes interacting with operations planners to marshal sufficient resources at one site or another. Because of the long planning phase and ever-changing operational demands, human resource needs are in a constant state of flux. Often, mobilization planners end up chasing down staffing numbers from the operations team to try to identify available human resources and quickly work out the details of how best to get staff to where they are most needed.

Mobilization planners need to interact with their counterparts handling training, transportation, and communication needs to determine where and when the security force will be welcomed to the event location, briefed on the security system, and outfitted with necessary gear upon arrival. Setting up rally points or welcome centers is a necessary part of the mobilization process and serves to set positive first impressions.

Planners must prepare for the arrival and processing of very large numbers of security staff, all scheduled to descend on the site within a short time frame. Because of the interdependent functions, it is useful for the relevant work teams to engage in joint tabletop exercises throughout the planning process to identify gaps and determine solutions.

5.2.1.3 INFORMATION TECHNOLOGY

Information technology (IT) aims to establish the best ways to store, retrieve, and send information throughout the security operation. It includes several key aspects and objectives.

- **Communication and IT design: establishing effective and secure radio, telephone, and other means of communication to all organizations and agencies involved in the security of the major event.**
- **Communication and IT controls: ensuring that power supplies can be maintained, command centers 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 for information flow so that everyone involved will know who should inform whom of what and when. Consideration should also be given to the management of data produced by systems, including feeds from CCTV cameras.**
- **Communication and IT protection: designing and implementing plans to protect core communications infrastructure such as cell towers and preparing plans to maintain communication in case of emergency situations such as terrorist attacks, violent protests, accidents, and natural disasters.**
- **Information management: using technology to manage plan development, exercise coordination, operations and administrative directives, and business rules or protocols concerning the release of information.**

5.2.1.4 RADIO COMMUNICATIONS

Radio communications pose particular challenges and risks. Early consideration should be given to system requirements, and a thorough assessment of existing infrastructure and equipment should be performed. Setting up a radio communication system for a major event can be a costly venture. In the case of new purchases, equipment needs to be tested at the earliest planning stage. Time needs to be factored in for contracts, procurement, training, deployment, testing, and retesting of these systems.

Radio transmission towers are a critical part of the communications infrastructure and represent a significant threat should any one of them be incapacitated. Planners need to ensure these structures are secured with suitable fencing, intrusion alarms, and even video monitoring.

Transmission frequencies will need to be assigned for each of the different chat groups within the wide spectrum of operational requirements, including land operations, air operations, marine operations, site security, specialized units, motorcades, close protection details, and more. Planners will have to ascertain different aspects specific to radio communications. For example, will encryption capabilities be needed to enable secure communication between these groups? Is there a national regulatory body that oversees the assignment of radio frequencies?

Additional challenges arise when multiple jurisdictions work together. Radio systems are often incompatible between different police services, a problem that can be exacerbated if there is a critical safety event that involves the deployment of fire and medical personnel. To bridge this gap, command centers often include a joint communications section where leads from different agencies coordinate their radio communications.

5.2.1.5 ACCREDITATION

The accreditation process is one of the cornerstones of security. By creating and implementing clear, standard procedures for determining who has access to a particular site—and who is not entitled to be there—the accreditation team provides a strong first line of defense. Everyone involved in security planning, including municipal, provincial, and federal partners, must understand the high stakes involved in the accreditation process in terms of the event's success or failure and subsequently the host nation's international reputation.

The security accreditation team will work closely with the event organizers to ensure a suitable, integrated process with legally based consent and privacy applications to allow for security background checks.

Accreditation will be required for:

- **Participants (such as delegates or athletes) and support staff**
- **Site staff/employees**
- **Media**
- **Security personnel**
- **Public safety personnel (fire, emergency medical services)**
- **Residents and their visitors within the controlled access or interdiction zones**

The security accreditation team's tasks include conducting appropriate searches of local, regional, national, and international police and security databases to establish the existence of any criminal history, criminal records, or intelligence records; facilitating the appropriate level of access credentials; and, in the case of an applicant's criminal or intelligence culpability, making recommendations with respect to the accreditation decision.

In some cases, such as certain international sporting events, the accreditation credential for the event also serves as an officially sanctioned entry visa for certain participants. In those cases, the credentials must be treated and secured as official government entry documents.

5.2.2 THE PROCUREMENT BRANCH

Before procuring any required equipment or services, the procurement branch will need to conduct an options analysis in order to consider opportunities to leverage existing assets to the fullest extent possible. This applies to goods and services that include, but are not limited to, temporary accommodations, long-haul personnel transportation services, rented or leased equipment or buildings, lighting, generators, and vehicles. Regardless of the procurement source (existing assets borrowing, leasing, or contracting), procurement personnel must identify when such assets will be required and consider such factors as the time it takes to go through a government procurement process and the capability of each supplier to deliver at scale. The risk of not doing this type of analysis is that operations personnel will not have the resources they need on time. Sufficient time should also be built in for testing new equipment and training users well in advance of the event.

Planners may also need guidance on with respect to developing statements of work and defining requirements for suppliers and vendors. Experienced procurement professionals need to be part of the planning team to develop requests for proposals, lead bid evaluations, and negotiate contracts as applicable.

5.2.2.1 PROPERTY ACQUISITION

Based on identified needs, the procurement group will develop options analyses related to the acquisition of real estate, related retrofits, and eventual decommissioning, complete with cost estimates. Collateral activities will include managing the planning and allocation of office space, building safety, and maintenance procedures.

Depending on the type and location of the event, property infrastructure requirements could include, but not be limited to, the following (see the Warehousing section below as well):

- **Office space for the integrated security unit**
- **A central command center**
- **Area command center(s), depending on the geographical size and scope of the event**
- **Communications equipment exchange and repair facility**
- **Land leased for radio towers**
- **Quartermaster stores facility**
- **Vehicle maintenance, repair, and fuel facility**
- **Staging facilities**
- **Helicopter landing zone and related petroleum, oil, and lubricant points**
- **Marine wharfs and related petroleum, oil, and lubricant points**

- Portable guard huts for theater of operations
- Stand-alone medical clinics at selected staging areas within the theater of operations
- Temporary housing facilities
- Cafeteria and common areas within close proximity of temporary housing facilities

5.2.2.2 GOODS AND SERVICES

Based on the requirements identified by the planning team, the procurement team should develop a plan to ensure that all goods and services are acquired in a timely fashion, in accordance with established government contracting policies and regulations. When and where possible, the opportunity for "joint procurement" with other government agencies or the event organizers should be considered to minimize internal competition, avoid duplication of equipment, and maximize volume purchasing power.

5.2.2.3 WAREHOUSING

The storage of goods and assets is an important component of the logistics pillar. Planners need to think in terms of the type and volume of assets and when and where assets will be needed for the planning, operations, and close-out phases. The scale of warehousing needs is often underestimated. Planners should take the time to determine warehousing requirements early on, before entering into contracts, to avoid wasting time and resources finding warehouse space that they will soon outgrow.

They should determine, for example, whether one large warehouse would be better for a specific purpose or whether it would make more sense to have multiple smaller warehouses strategically located throughout the security footprint. There will be a need to store all sorts of assets and supplies that enable security planning, everything from office furniture and computers to paper and pens. If there will be motorcades, planners must determine how many vehicles will be required, when they will be received, where they will be outfitted with emergency equipment, and then where they will be securely stored until they are ready to be used.

As the event nears and forces begin to mobilize, assets such as generators, staff cars, equipment and clothing, bottles of water, bug repellent, boxed lunches, notebooks, portable radios and batteries, and much more will need to be dispersed from accessible locations. One very important consideration is the storage of hazardous materials such as firearms, ammunition, fuel, or crowd control gas. How will these materials be stored? Are local permits required? Who is qualified to manage the storage and distribution requirements?

Warehouse security is another consideration. Is the building physically secure? Are repairs needed before entering into a contractual agreement? Consider the need for external fencing, lighting, alarm systems to warn of intruders or fire, and video cameras.

Lastly, when entering into contracts, planners need to ensure they allow sufficient time after the event for the return and cataloging of assets for long-term storage or disposal. This process often takes longer than first anticipated.

5.2.2.4 ASSET MANAGEMENT

A system to help manage the inventory of physical assets—including arrival, distribution, tracking, and reporting—is crucial. There are several suitable off-the-shelf solutions that can be used during a major event; however, they should have a network application with a central server, enabling many users to access the data. Handheld computers or smartphones enable data from QR codes, barcodes, or radio frequency identification tags to be collected easily, quickly, and accurately, then analyzed and reported on as needed. The system should have comprehensive import and export capabilities so that information can be readily exchanged with backend systems such as SAP, Oracle, or others. Planners may also wish to take advantage of recent cloud technology developments as well.

Planning should include the creation of a workforce welcome/farewell center where incoming and outgoing personnel can be issued returnable or single-use personal equipment (everything from radios to sunscreen) for the duration of the event. These centers can also be used as orientation and briefing areas as personnel arrive and depart the event.

5.2.2.5 ACCOMMODATIONS

Accommodations for the event security personnel should be rented or leased in centralized locations as close as possible to the work sites. Where possible, acquisition of appropriate accommodation should be coordinated through an accommodations manager and team. Some of the considerations that will need to be addressed include:

- **Cost**
- **Location and quality available near the theater of operations**
- **Timelines required to establish and dismantle any temporary accommodations**
- **Security measures at housing locations**
- **Transport scheduling**

5.3 COMMUNICATION

The communication pillar has two categories of outputs: internal and external communication plans. External communication should include plans for media and community relations as well as the use of social media. Because the lines between external and internal communications are increasingly blurred in today's social media-driven world, the plans should be aligned to allow natural crossover.

5.3.1 INTERNAL COMMUNICATION

Effective internal communication within and across the organizations and agencies involved in the security of a major event will go a long way toward strengthening coordination among different teams. It allows authorities to disseminate information, keep everyone up to date, clarify what is expected in operational terms, and reinforce mission objectives. Planners need to be both informed and consulted about decisions, which means two-way internal communication is needed. An effective internal communication process will set the stage for professional external communication on security matters.

Personnel should consider how to ensure that the information being disseminated across different channels and partner agencies is consistent and up-to-date and how to avoid pitfalls such as duplication of information or communication silos. Having a shared, efficient, robust platform that allows all pillars of the security operation to talk to each other is also essential. The platform must be secure and interoperable, with encryption capability for transmitting sensitive or classified information when necessary.

5.3.2 EXTERNAL COMMUNICATION

Major events tend to attract a great deal of media attention, some of it not entirely complimentary. An effective external communication strategy has the potential to enhance public confidence and minimize potential harm to the reputation of the event security organizers.

5.3.2.1 COMMUNICATION WITH THE PUBLIC

A strategy to communicate with the public is paramount during all stages of a major event. *The Guide on the Security of Major Sporting Events* lists examples of what a public communication strategy should accomplish and when:

- **During the Exploratory and Bidding Phases it should help to create momentum, enthusiasm, engagement and a common sense of purpose within the community;**
- **During the Planning Phase it should maintain momentum, popular and political support, and create transparency as to how public resources are being used;**
- **During the Implementation Phase, a good external communication strategy should keep spectators and staff properly informed, which can also contribute to better surveillance and detection of threats; and**
- **During the Post-event Phase, it should communicate the positive impacts of the [major sporting event] on the community and host authorities.**[35]

It is important to be able to communicate seamlessly with various target audiences in the most appropriate way. As with the other elements of security planning, the communication strategy should take a whole-of-government approach and also include other partners. The security operation should establish an integrated security communication team (ISCT) to ensure consistency of messaging, especially given all the different agencies, organizations, and companies involved in a typical major event. This centralized approach will reduce the risk of having too many spokespeople or public-facing communication channels.

This centralized communication team should establish and maintain open dialogue with the public, business community, activist groups, and the media to address concerns and build a shared purpose in support of an event that is peaceful and safe for everyone. To do that, it will be essential to promote a strong communication partnership among the participating security, government, organizing committees, and corporate partners.

5.3.2.2 SOCIAL MEDIA

Social media has become a powerful tool for reaching diverse audiences, including when it comes to conveying information about security measures. Furthermore, through frequent communication on social media platforms, the ISCT can maintain an ongoing dialogue with the public and thereby build community trust, which in turn enhances security.

35 *Guide on the Security of Major Sporting Events: Promoting Sustainable Security and Legacies*, p. 130.

The ISCT should take full advantage of externally facing websites and social media platforms to keep the general public, demonstrators, the media, spectators, local businesses, and other stakeholders informed about security measures. This should include information about how the event will unfold and how each step will affect the public, for example in the case of road closures, special public transportation arrangements, and legal measures in place during the event. The social media team is able to monitor Twitter trending using tools that give real-time updates on all posts. This enables the team to see what users are talking about (true or untrue), where certain events are happening, and what groups are attending. With this information, the team can enhance situational awareness of current events, forward information to a unified command center, and take any appropriate action to correct misinformation or react to developments. Using social media effectively is about more than posting messages on the Internet; it's a way to understand how people are thinking about events, which enables the communication team to develop more effective messages.

> Web exchanges in social media allow interpretation of the public mood and can, to some extent, even predict people's likely behaviours in certain situations. By leveraging social media, planners can gain greater situational awareness and enhance communication strategies. Social media monitoring should always be conducted within the confines of the law and with due respect for existing privacy regulations.[36]

5.3.2.3 MEDIA RELATIONS

The mainstream media has the ability to influence public perception of the security process positively or negatively. There must be a strategy to keep the local, national, and international media informed about the event and address local concerns about how the event might affect the community. A media strategy should include the following components:

- **Relationship building**
- **Technical briefings**
- **Proactive media interviews**
- **Timely reactive media interviews**
- **Provision of photos and videos**
- **Detection and correction procedures to counter misinformation**
- **Comprehensive one-stop website**

During the event itself, ISCT team leaders and public affairs staff should be deployed at key locations to be available to local security commanders if needed.

36 *Guide on the Security of Major Sporting Events: Promoting Sustainable Security and Legacies*, p. 130.

5.3.2.4 COMMUNITY RELATIONS

One important element of the communications strategy should be to create a community relations group (CRG) to establish and maintain open and transparent lines of communication with all stakeholders who may be affected, directly or indirectly, by the event. The CRG should build a relationship of trust, mutual understanding, and respect, engaging with community organizations, local businesses, municipal governments, emergency services, local associations, and protesters. Establishing mechanisms for dialogue with these groups and keeping them apprised of the event and its likely impacts can help improve specific aspects of security planning and operations. It is important to have personnel on the CRG who have current knowledge of the local community and understand the social, economic, and political dynamics, nuances, and tensions. A respectful ongoing dialogue with activists is also encouraged, one that recognizes their rights to protest and advises them of security expectations, actions, and consequences. A community activist liaison can help forge an agreement about designated protest areas.

The CRG can also canvass local communities as a source of knowledge on vulnerable groups, such as persons with disabilities who should be considered during crowd management or at security checkpoints.

5.4 CONTINGENCY PLANS

Contingency plans are supplementary to the outputs and can be considered specific alternatives to the operations, support and communication plans. As such, they are a shared responsibility of multiple stakeholders.

Contingency planning envisions the worst that could happen. The consequences of an incident caused by a terrorist attack, cyberattack, public disorder, natural disaster, major accident, man-made emergency, disease outbreak or other such occurrences could be catastrophic, so security planning must consider all such eventualities. Contingency plans are designed to respond to repercussions of an unplanned event by:

- **Saving and protecting life and property**
- **Treating, rescuing, and transporting casualties**
- **Containing the emergency and the casualties**
- **Managing evacuations**
- **Cancelling or stopping the event**
- **Safeguarding the environment**
- **Maintaining critical services**
- **Providing the media with information**
- **Restoring normalcy as soon as possible**
- **Ensuring scenes and evidence are preserved**
- **Facilitating investigations and inquiries**

Contingency plans should have a comprehensive, all-hazards approach that ensures a coordinated and organized response to any emergency, including disease outbreaks and extreme weather. Security planners need to design robust, cohesive contingency plans and make sure that there are management systems built to execute and control effective responses.

CONCLUSION

The purpose of this manual is not to teach planners how to plan but rather to offer a user-friendly format that helps identify and organize the main components of the security planning process. Much of the information contained here is designed to stimulate thinking about the full scope of considerations that go into a security plan for any major event or any situation that might involve crowded public places or other vulnerable targets. Each event and each place will be subject to different conditions and constraints depending on the local environment.

The SIPOC model—with its analysis of sources, inputs, process, outputs, and customers—is just one of the tools planners could use to organize their operations. It has the advantage of offering a methodological structure while being flexible enough to adapt to different circumstances.

This manual focuses on the first four components of the SIPOC model, but it is important for planners to remember that all the work of security planning ultimately must benefit the end users, the customers. In this context, that category includes not just event-goers but the public at large, both visitors and local citizens who are the raison d'être of the entire operation and who deserve to have their safety and security made the top priority.

It is with those customers in mind, too, that Chapter 1 of this manual focuses on the guiding principles that must anchor any security operation: human rights, gender equality, and environmental sustainability. Those people-centered values, combined with the methodical work of planning, will enable planners to stage a successful and safe event.

Through this manual, the OAS/CICTE and UNICRI hope to contribute to the knowledge and resources available on this topic and provide further support to countries looking for additional guidance and consultation. The manual is intended to be considered within the broader structure of the OAS/CICTE and UNICRI technical assistance framework. Through this initiative, planners can benefit from a large database and broad network of national governments, organized by the relevant expertise of their representatives and by the different elements of security planning. Such a broad networking platform is essential to help beneficiaries implement technical tools as well as to assist them in developing and adopting common policies.

Security planning is not something any government needs to take on alone. The central role of international cooperation in this task cannot be underestimated. At a time when security risks are increasingly global, countries must work closely together to address these concerns and create a safer environment.

OAS More rights for more people

unicri United Nations Interregional Crime and Justice Research Institute

Security Planning on a Large Scale:

A Practical Manual