Safety, Security, and Service: A Practitioners Toolkit for Major Events in Cities

2025

Major Event Definition

Following the United Nations Interregional Crime and Justice Research Institute (UNICRI) International Permanent Observatory (IPO) on Security Measures during Major Events definition, a major event can be considered as a foreseeable event that should have at least one of the following characteristics: *Historical, political significance or popularity; large media coverage and/or international media attendance; participation of citizens from different countries and/or possible target group; participation of VIPs and/or dignitaries; or high numbers of persons.* These characteristics also apply to large events at a city-level and, therefore, this resource is intentionally generic to encompass both major and large events, and those that are closed (venue specific) or open (in public areas) by nature.

Protective Security

Protective security is concerned with the protection of information, people, and physical assets. It comprises the governance arrangements, mitigating policies, infrastructure, and operations required to counter a range of threats and protect assets from compromise. In the context of events, this includes venue or footprint security, and that of participants/spectators.

Aim and Purpose

This toolkit is a short aide memoire that aims to promote a proactive and accountable approach towards enhancing safety and security at major events. Its purpose is to offer an easily digestible and practical guide that summarises generic overarching considerations.

It is formatted as a checklist that consolidates key steps from assessing threats and enhancing protective security measures to managing event operations in a safe and secure way. These are intended to be headline bullet points that signpost readers to more detailed resources.

Disclaimer: This toolkit has been developed by the Counter Terrorism Preparedness Network and INTERPOL Project Stadia in consultation with expert working groups and specialist agencies. However, the content is non-exhaustive and may be applied in different ways subject to local laws, contexts, and circumstances. It is the responsibility of the relevant authorities to ensure proportionate, legal, accountable, necessary, and ethical approaches that enable safe and secure event operations. At the time of release, all identified resources and their respective hyperlinks were working properly. However, this may change over time as each resource is maintained independently of this document.

Overarching Considerations

1. **Develop a Security Strategy and Governance Structure**

   Utilise security legislation and regulations at international and national levels to inform those at the regional, city, or local level. This can help drive a policy-approach towards an event (what needs doing and why) and the strategy (high-level vision, objectives, and who does what and how, in line with the policy in place).

   The security strategy should be overseen by a senior officer, with the knowledge, experience, and authority to ensure a clear direction is set in terms of strategic intent, expectations, and risk acceptance. Robust governance arrangements must subsequently ensure accountability for the maintenance and delivery of the strategy.

This should translate to, and dovetail with, the plans, procedures, or operating frameworks of public authorities and event companies including at specific sites or venues. Police services and other public authorities will routinely work within pre-established arrangements and structures, and event organisers/venues should ensure that they align with these for a coherent and coordinated approach at the tactical and operational levels.

It is important that priorities and approaches towards public communications are considered. Public communications can constitute security-minded or deterrent communications and should complement emergency management plans. This must recognise specific nuances around the event as well as the wider area. This is referred to by INTERPOL Project Stadia and others as the spectator journey, which includes acknowledging the transport hubs and systems, hotels, and hospitality services, as well as the wider businesses and city infrastructure that those attending may use.

- Australia's Counter-Terrorism Strategies.
- Government of Western Australia (2022). Guidelines for Concerts, Events, and Organised Gatherings.
- INTERPOL Project Stadia (2023). Key Considerations for Securing Major Events.
- INTERPOL Project Stadia (2023). Hosting Major International Sports Events (not available online).
- OEA/UNICRI (2022). Planificación de Seguridad a Gran Escala: Un Manual Práctico.
- Swedish Civil Contingencies Agency (2021). Event Safety Guide.
- UK National Protective Security Authority. Built Asset Security Strategy Template.
- UK National Protective Security Authority. Developing a Security-Mindedness Approach.
- UNICRI (2007). IPO Security Planning Model.
- United Nations (2021). Guide on the Security of Major Sporting Events.

2. Assess Threats and Vulnerabilities

Conduct a full threat and vulnerability assessment of both the event footprint and venue to map and identify security priorities. Understanding the event profile (e.g., history, type, and visibility of the event, audience profile, expected numbers, associated political sensitivities or trends etc.) will inform the planning process. Likewise, analysing venue vulnerabilities and gaps in terms of safety and security will inform mitigation measures. The 'EVILDONE'* (Exposed, Vital, Iconic, Legitimate, Destructible, Occupied, Near, and Easy) mnemonic offers a framework for assessing the vulnerability of targets.

Other mnemonic tools like 'CARVER' (Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability) or 'PESTLE' (Political, Economic, Social, Technological, Legal, and Environmental) can support this process but should always be accompanied by advice from police services as appropriate.

This may include specialist advice relating to counter terrorism. In this context, explicit reference to attack methodologies, likelihood, and the events vulnerability to them, should be included. This leads to threat-based planning assumptions, where the specifics of a potential attack are considered and planned for. The development and implementation of a threat mitigation strategy should follow, addressing those identified internally or externally. A consistent, comprehensive, and auditable approach should be applied.

This should cover all elements of the event from crowd capacity and movement; access/egress; to protective security. This will inform mitigation measures and the strategic placement of resources from equipment to specialist operational units.

- The Governance of Security and the Analysis of Risk for Sporting Mega-Events: Guidance Notes for Security Planners.
- The National Center for Spectator Sports Safety and Security NCS4 (2024). Venue Security Director Survey.
- Office of Community Oriented Policing Services, U.S. Department of Justice (2008). Policing Terrorism: An Executive's Guide, COPS Centre for Problem-Oriented Policing.*
- PooleRe. Vulnerability Self-Assessment Tool.
- Protect UK (2024). Standards for Public Access Trauma (PAcT) First Aid Kit.
- Safe Stadium (2024). CBRN Security of Mass Events Checklist (availability per request to the Project Safe Stadium).
- US Secret Service National Threat Assessment Centre (2023). Mass Attacks in Public Spaces 2016-2020.

3. Integrate Layered Protective Security

Implement protective security measures and arrangements (mobile and static; covert and overt; hard and soft) at the venue and in the vicinity of the event where legal to do so. This ranges from and is not limited to control measures such as signage to deter criminal or malicious acts to surveillance, hostile vehicle mitigation, other physical or implied barriers, security staffing, body/bag searches, gate systems, and ticketing control. The '4Ds' - Deter, Detect, Deny, Delay – apply, as do mechanisms for response and recovery.

The principle is building defence through depth. The UK National Protective Security approach on layers, 'beyond the perimeter', 'the perimeter', 'within a site', and 'critical assets of the site', and the 'Swiss-cheese' model, offer useful ways to understand this.

Outer and inner perimeters can be applied alongside careful route management that guides the flow and concentration of attendees. In some cases, this could be enhanced by phased queuing and entrance times. These techniques are utilised to keep people moving to avoid overly dense footfall, or pinch-points and bottlenecks that could carry risks or become targets. The potential aerial threat posed by drone-enabled surveillance, hostile reconnaissance, or the delivery of weaponry or explosives also need to be accounted for.

Consideration can also be given to the use of drones in security, as well as the integration of technology more broadly. Artificial Intelligence, for example, could offer options relating to biometrics like facial recognition (where authorised); alerts if marked individuals, weapons, or suspicious/violent behaviour is identified; and the ability to monitor crowd movement and enhance situational awareness. Likewise, drones can be deployed for monitoring, surveillance, and to live stream footage as appropriate (where authorised).

It is otherwise important to recognise who has responsibility and if there is a transition of responsibility, for example when a private event venue merges into local authority land. It is equally important to recognise and address any grey areas. These are areas where there is a degree of uncertainty around who is responsible and should lead on the safety and security of that space. These considerations should fall into the decisions of the designated strategic commander who should be seeking professional counsel from partners, other lead public-sector agencies, and experts as part of this role.

- ANZCTC (2023). Active Armed Offender Guidelines for Crowded Places. Australia-New Zealand Counter Terrorism Committee, Commonwealth of Australia.
- ANZCTC (2023). Chemical Weapons Guidelines for Crowded Places. Australia-New Zealand Counter Terrorism Committee, Commonwealth of Australia.
- ANZCTC (2017). Hostile Vehicle Guidelines for Crowded Places. Australia-New Zealand Counter Terrorism Committee, Commonwealth of Australia.

- ANZCTC (2023). Improvised Explosive Device Guidelines for Crowded Places. Australia-New Zealand Counter Terrorism Committee, Commonwealth of Australia.
- Australian Government (2018). Crowded Places Checklists, Australian Institute for Disaster Resilience.
- Counter Terrorism Preparedness Network (2023). City Preparedness for Cyber-Enabled Terrorism.
- Counter Terrorism Preparedness Network (2024). Preparing for Hostile Drones in Urban Environments.
- Counter Terrorism Preparedness Network (2019). Protecting Major Events and Crowded Places Report (not available online).
- CISA (2024). Mass Gathering Security Planning Tool.
- CISA (2019). Security of Soft Targets and Crowded Places Resource Guide.
- European Commission (2023). Protection against Unmanned Aircraft Systems.
- European Commission (2022). Security by Design Protection of Public Spaces from Terrorist Attacks.
- INTERPOL Project Stadia (2023). Stadia Protection and Mitigation from Drone Incursions and Threats: Guidelines for Testing and Evaluation of Counter Unmanned Aircraft Systems (C-UAS) Capabilities.
- RAND Homeland Security Operational Analysis Centre (2024). Improving Security of Soft Targets & Crowded Places.
- Safe Stadium (2024). CBRN Security of Mass Events - Procedures, Tools, Plans and Guidelines (availability per request to the Project Safe Stadium).
- UK National Protective Security Authority. Build it Secure and Physical Security Guidance.
- UK National Protective Security Authority (2024). Mitigation of Terrorist Threats at Venues during Ingress & Egress.
- UK National Protective Security Authority (2018). Protective Security Management Systems.
- United Nations (2022). Protecting vulnerable targets from terrorist attacks involving unmanned aircraft systems (UAS).
- United Nations and INTERPOL (2022). The Protection of Critical Infrastructure Against Terrorist Attacks.
- United Nations E-Learning. Vulnerable Targets Protection on the Occasion of Major Sporting Events.
- United Nations Office of Counter Terrorism (2022). Protecting Vulnerable Targets Against Terrorist Attacks: Good Practices.

4. Establish Security Operations, Emergency Response, and Crisis Management Plans

Undertake online vulnerability assessments (an assessment of how the event appears on open source and how any aspect of it may be used during online hostile reconnaissance) and on-site vulnerability assessments (utilising venue blueprints or mapping tools to inform planning). Blueprints, aerial maps, or more advanced digital twin technology can be used to sectorise a site for the purposes of managing security operations and informing a wider emergency response. They can also help with identifying access and egress points, understanding the flow of people around an event site, and other risks/hazards.

Plans should consider secondary attacks, or subsequent incidents such as crushing, inside or outside an event site. Understanding the potential consequences of one or multiple attacks, and how they would be managed, is critical. This relates to the capabilities and coordination of multi-agency partners at strategic, tactical, and operational levels.

Plans must contain clear and agreed activation protocols and processes; key contacts; steps and needs to consider. They should include pre-identified rendezvous points for emergency services, spaces for supporting the public, and potential routes for dispersal.

Communications will also need to be a core consideration. This may warrant public messaging and signage before, during, and after the event, which can incorporate safety and security campaigns. Apps and alert systems can also be used.

All plans should be consulted with multi-agency partners, reviewed on an ongoing basis via a Safety Advisory Group or equivalent, and embedded through training and exercising. It is also a good practice to submit plans to peers review.

- CIPR & CPNI (2019). Crisis Management for Terrorist Related Events.
- CISA (2008). Evacuation Planning Guide for Stadiums.
- Counter Terrorism Preparedness Network (2019). Strategic Coordination.
- Economic and Social Research Council (2023). Public Behaviour in Response to Perceived Hostile Threats.
- FEMA (2017). National Incident Management System (Third Edition).
- Police Executive Research Forum (2011). Managing Major Events: Best Practices from the Field.
- Police Foundation (2018). Managing Large-Scale Security Events: A Planning Primer for Local Law Enforcement.
- Safe Stadium (2024). CBRN Security of Mass Events, Evacuation and Crowd Management Guidebook (availability per request to the Project Safe Stadium).
- UK Government. Joint Emergency Services Interoperability Principles.

5. Ensure Vetted, Trained, and Security Aware Personnel

Appropriate staffing is vital for the safe and secure delivery of any event. This may include volunteers, safety stewards, licensed security officers, close protection operatives or teams, as well as the police. This should range from static and mobile to covert and overt operatives. High-visibility officers can support threat deterrence and can be prepared to respond and provide first aid, for example, whilst low-visibility officers may be well placed for monitoring behaviours, carrying-out surveillance, and to intervene should any issues arise. Officers could also be proactively deployed to at-risk areas or CCTV blind-spots.

Whether volunteers or private security personnel are available in-house or provided by an external supplier, security must be trusted and accredited, with industry standards and an audit trail to match. A robust recruitment process and enhanced vetting coupled with role-specific training, supervision, and the ongoing monitoring of performance is essential.

This demands strong policies, governance, and leadership; insider risk assessments and pre-employment screening; ongoing personnel security; monitoring and assessment of employees; responsive investigation and disciplinary processes; as well as a progressive approach towards driving security culture and behaviour change that has a positive influence on practices. Collectively, this can reduce the insider threat and drive effectiveness in security operations.

Superficial searches, for example, need to be avoided. Searches upon entering an event should be thorough and conducted as far as necessary (and legally) to fulfil whatever the search objectives are. Enhanced searching equipment including screening arches may be required. Body worn cameras can be a useful way of encouraging appropriate conduct and capturing evidence. Assurance should be actively sought through clear supervisory structures as well as regular and random checks and tests by independent evaluators posing as attendees. The practice of exercises using red teaming (where various tactics, techniques, and procedures are used to mimic how real attackers might operate) can also detect gaps in the security plans or ameliorate responses.

- CISA (2021). Public Venue Security Screening Guide.
- INTERPOL Project Stadia (2022). Guide to Stadium Safety, Security Licensing and Certification.
- Protect UK. ACT Awareness E-Learning Package.
- UK National Protective Security Authority. Role Based Protecting Security Risk Assessment.
- UK National Protective Security Authority (2024). Security Culture Tool.
- UK National Protective Security Authority. Embedding Security Behaviours: A framework for improving security behaviour within organisations.
- UK National Protective Security Authority. Personnel Security Maturity Assessment Tool.

6. Demonstrate Compliance with Standards and Best Practices

Pre, during, and after an event, organisers should be able to clearly demonstrate how they have done everything reasonably and practicably possible to make the event safe and secure. All those involved in event safety and security should be able to demonstrate how they have prioritised this and invested in threat mitigation measures as required.

There should be records of how these measures meet standards, when lead authorities and security experts were consulted, and how learning from attacks at events has been considered and applied in full. Event organisers must be able to justify how the safety and security arrangements for their events are properly informed and appropriately developed in proportionate, legal, accountable, necessary, and ethical ways.

- Events Safety Industry Forum, Purple Guide.
- ISO 22341:2021 (2021). Security and resilience — Protective security — Guidelines for crime prevention through environmental design.
- ISO 22342:2023 (2023). Security and resilience — Protective security — Guidelines for the development of a security plan for an organization.
- ISO 22343-1:2023 (2023). Security and resilience — Vehicle security barriers.
- ISO 22379:2022 (2022). Security and resilience guidelines for hosting and organizing citywide or regional events.
- ISO/IEC 27001:2022 (2022). Information security, cybersecurity, and privacy protection — Information security management systems — Requirements.
- The National Center for Spectator Sports Safety and Security. NCS4, Publications.
- UK Sports Grounds Safety Authority. Green Guide.