



# Event Security & Counter Terrorism Guidance

# Event Security & Counter Terrorism Guidance

31 August 2023

## Introduction

Event organisers have an obligation under the Health and Safety at Work etc Act 1974 to provide a safe place for their employees to work and environment for attendees. This includes consideration of foreseeable security risk and the appropriate measures needed to manage the exposure to risk.

The objective of this document is to provide a best-practice guide to industry colleagues who are responsible for planning and delivering organised events, trade shows and exhibitions of all sizes, in all UK locations.

We believe in order to do this we must work collaboratively with our stakeholders to ensure the security considerations and measures we have in place are practical, appropriate, effective, responsive and considered best practice for the industry. Communication is a critical success factor in this program achieving its overall objective to provide assurance and build confidence for all people who participate in and visit our organised gatherings.

It may not be required, nor possible, to execute every action, and so these principles are designed to encourage focus on appropriate security measures. In some instances, security measures will be mandated or prescriptive and, in such cases, will be followed as a minimum guideline.

This document outlines **What** measures show organisers are taking to ensure the security of all visitors, exhibitors, contractors and staff, **How** these measures can be implemented, and **Why** it's an important component.

This guidance has been prepared by a group of Association of Event Organisers (AEO) organiser members in line with guidance published by [ProtectUK](#), [NPSA](#), advice from the event industry [MASA](#) (Multi Association Security Awareness) Group and other reputable sources.

It has been agreed at an event industry association level that the event venue will be responsible for providing a suitable level of campus security infrastructure, planning and control measures. Where an event may create a higher security requirement this will need to be discussed and agreed between the venue and the event organiser. If there are co-located events affected by a higher security risk event the venue would coordinate between organisers to plan and put in place the appropriate additional security control measures required. When an event is in a dry hire venue, greenfield or similar, the organiser may need to assume a higher level of responsibility for the security planning and arrangements.

The guidance in this document is based on information currently available and it is expected that the content may need to be adjusted accordingly once further details of Martyn's Law (formerly known as Protect Duty, also known as Terrorism (Protection of Premises) Bill) becomes available. One of the requirements of a Martyn's Law is that any measures should entail minimal new costs or burden.

It is important to remember that any security measures or plans do not conflict with health and safety requirements and fire regulations.

This document is designed as initial guidance only and event specific detail would be hard to prescribe due to the variety of event styles, locations, management structures. Where further guidance or more in-depth processes/ documents are required, this document should be interpreted and implemented by individuals for their own specific business and event needs. It is recommended that any additional advice is provided by a reputable security professional or counter terrorism specialists. NaCTSO are currently developing a Competent Persons Scheme (CPS) which will include the Competent Person in the Workplace (CPIW) approved qualification and a Counter Terrorism Security Specialists Register (CTSSR).

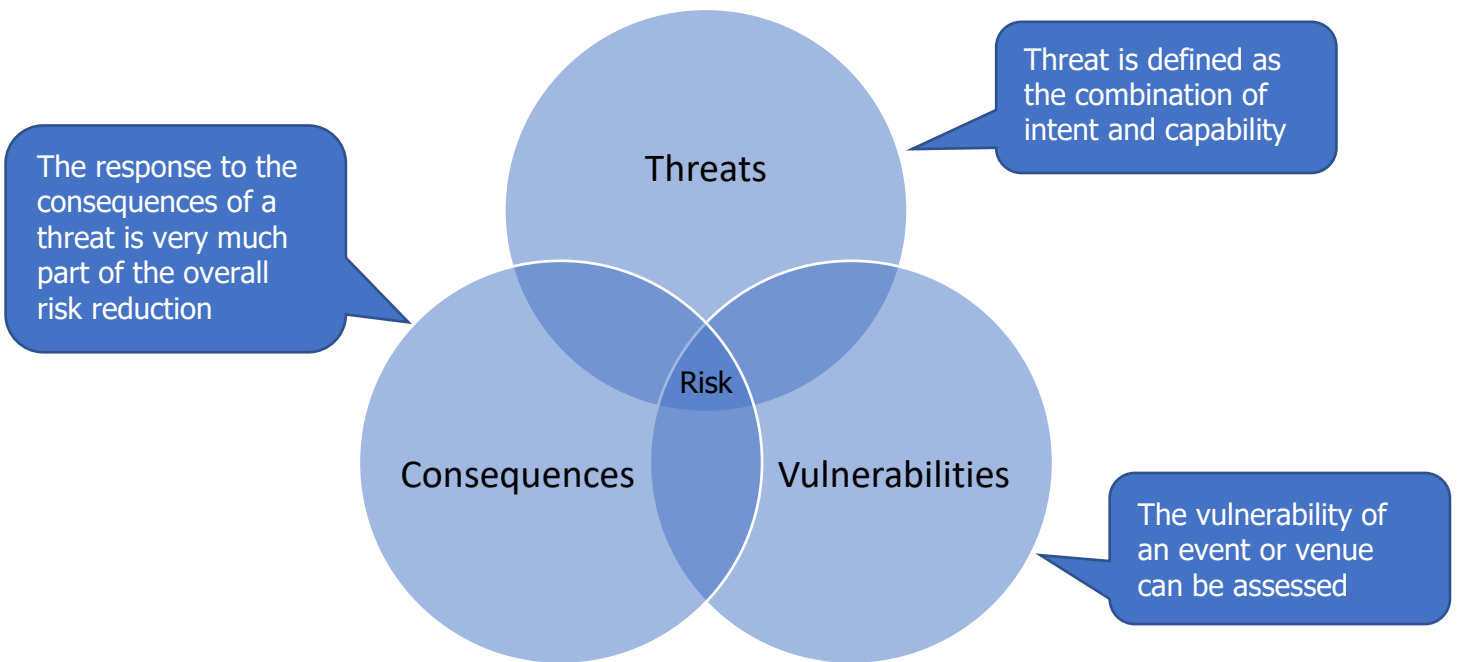
# Definitions

## Acronyms

There are various acronyms used within the security and counter terrorism subject, [Appendix 1](#) details some of the commonly found examples.

## Risk

Security risk is not the same as safety risk, often the security threat is not something that can be appropriately measured specific to an event therefore the UK threat level is applied.

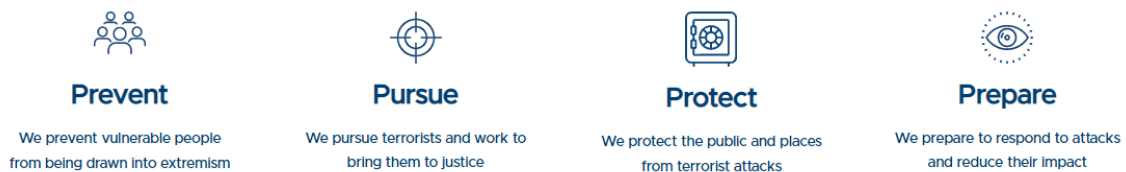


## Threat Spectrum

The threat spectrum would include physical, personnel and people, and how these threats might overlap or evolve over time.

## CONTEST - Prevent, Prepare, Protect and Pursue\*

[CONTEST](#) is the UK Government's counter-terrorism strategy and aims to reduce the risk from international terrorism so people can go about their daily business. Developing and delivering CONTEST involves numerous stakeholders, including government departments, the emergency services, voluntary organisations, the business sector and overseas partners. The strategy is divided into four principal strands: [Prevent](#) [Pursue](#) [Protect](#) and [Prepare](#).



**Prepare** involves planning for and responding to an attack with the aim to reduce the impact.

**Protect** is based on controls around crowded places/ publicly accessible locations and includes [Project Servator](#). Project Servator is a policing tactic that aims to disrupt a range of criminal activity, including terrorism, while providing a reassuring presence for the public.

\* The Prevent & Pursue are not relevant for this guidance and are therefore not covered further

# Event Security & Counter Terrorism Guidance Cornerstones

The guidance is based on the four cornerstones approach with additional details on each provided in the following sections:

## 1. Assessment

- 1.1. National threat level
- 1.2. Venue/ location risks
- 1.3. Event specific threat
- 1.4. General Event Security Risk Assessment
- 1.5. Counter Terrorism Risk Assessment (CTRA)

## 2. Planning

- 2.1. Vulnerabilities
- 2.2. Responsibilities
- 2.3. Competence

## 3. Control Measures

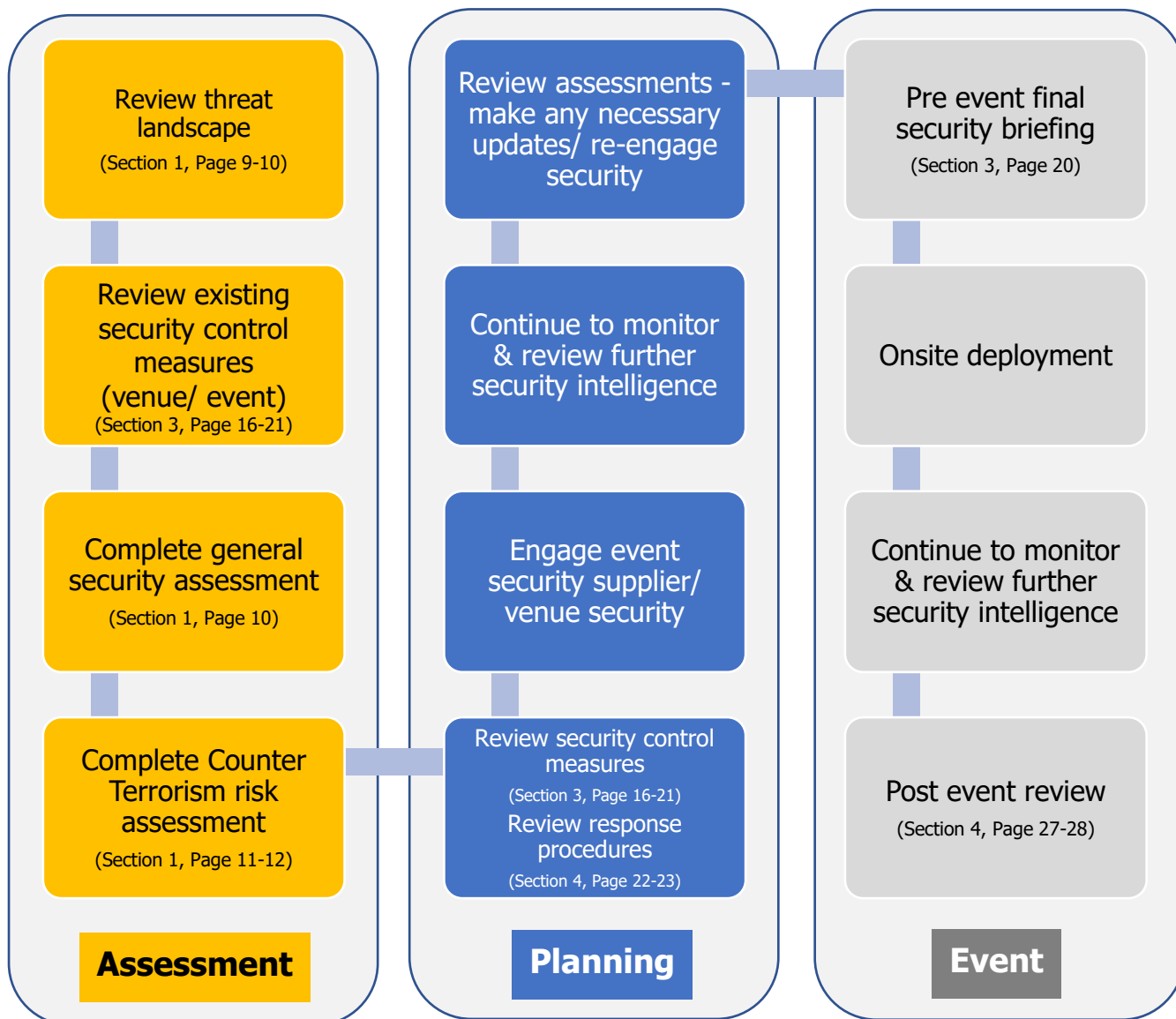
- 3.1. Layered Security Measures
- 3.2. Vulnerable Groups
- 3.3. Special Event Activities
- 3.4. Reporting Suspicious Behaviour/ Occurrences
- 3.5. Event Communication

## 4. Response/ Recovery

- 4.1. Critical Incident Management Plan
- 4.2. Procedures
- 4.3. Response Communication
- 4.4. Review



## Work Flow

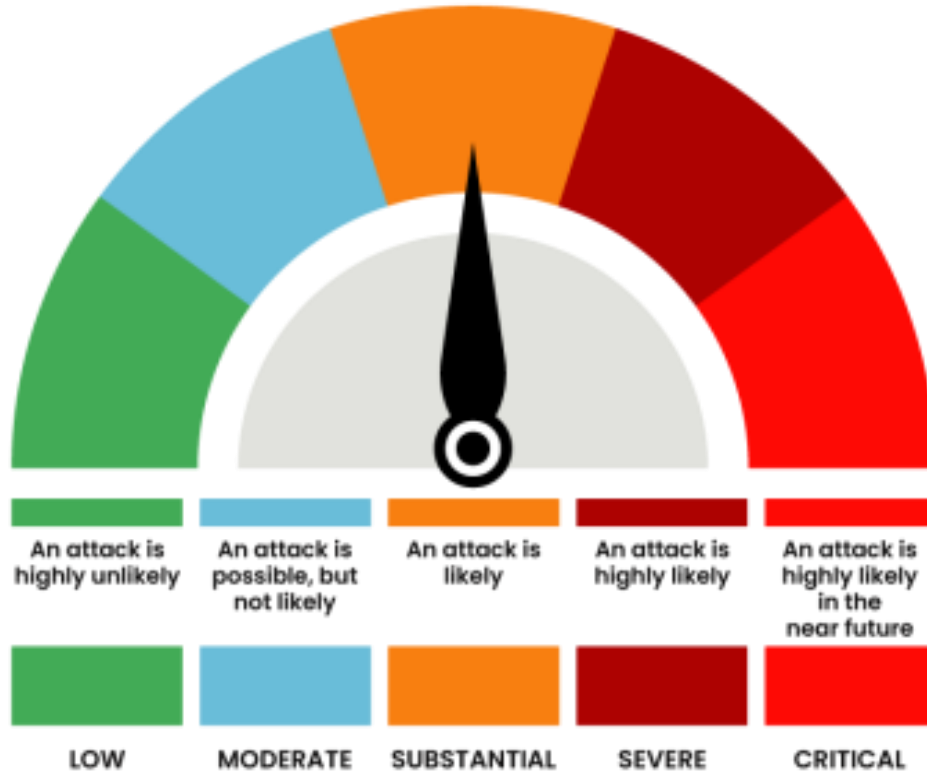


# 1. Assessment

## 1.1. National Threat Level

The event assessment security level should be reviewed in conjunction with the current UK Threat level when considering what response level to security planning and control measures are required.

The Joint Terrorism Analysis Centre (JTAC) sets the national threat level to help the public plan for appropriate levels of security. The decision is based on available intelligence, terrorist capability, intentions and timescale. Click [here](#) for more information.



As of March 2023

Further latest information on the threat level to the UK click [here](#).

### Previous National Threat Levels since July 2019

Date	Threat Level	Reason for raised threat level
9 February 2022	SUBSTANTIAL	
15 November 2021	SEVERE	14 Nov Liverpool (bomb)
4 February 2021	SUBSTANTIAL	
3 November 2020	SEVERE	Increase of jihadist terrorism attacks in Europe 29 Oct France (stabbing) 2 Nov Austria (mass shooting)
4 November 2019	SUBSTANTIAL	

It is considered unrealistic to maintain the highest severe or critical threat level for a prolonged amount of time. The threat level was previously critical in September 2017 (Parsons Green tube) and May 2017 (Manchester Arena) and remained at critical for just a few days.

It is suggested that instead of trying to deal with 5 individual levels of threat that the event industry can work within 3 levels: Exceptional, Heightened and Normal. This allows for planning within the Substantial/ Severe landscape which has been seen in recent years.

UK Threat Level	Description	Event Response Level	Description
Critical	An attack is highly likely in the near future/ expected imminently	Exceptional	Maximum protective security measures to meet specific threats and to minimise identified vulnerabilities and risk
Severe	An attack is highly likely	Heightened	Additional and sustainable security measures reflecting the broad nature of the threat combined with the identified specific vulnerabilities and judgement on acceptable risk
Substantial	An attack is likely/ a strong possibility		
Moderate	An attack is possible, but not likely	Normal	Routine protective security appropriate to the event vulnerabilities and judgement on acceptable risk
Low	An attack is highly unlikely		

The event security threat review, event security measures and event Counter Terrorism Risk Assessment (CTRA) should always be reviewed when the UK threat level changes. This review should be documented/ recorded. Existing planned mitigations may still be appropriate.

## 1.2. Venue

There is an expectation from organisers that a venue should have reasonable base security mitigation measures in place, for example:

- a current and appropriate security threat risk assessment and counter terrorism risk assessment (CTRA) that they can share and/ or discuss with the organisers
- physical measures and associated policies and processes in place to control access to the site by vehicles and pedestrians
- a nominated person responsible for security management and assessment of vulnerabilities and response plans
- collaboration with local police services and where necessary CT SecCO/ CTSA
- active and/ or reactive security monitoring in place, with appropriate staffing, to detect and/ or support intelligence gathering, such as surveillance, target acquisition and reconnaissance
- should share gathered and supplied intelligence which would need to be considered with the planning of the event security
- demonstrable consideration and assessment of measures in place to reduce the risk of vehicle as a weapon attack both within and on the approach to the site. This protection should include an appropriate mix of hostile vehicle mitigation, traffic control measures and deterrence
- reasonable measures in place to minimise the vulnerability of their critical assets (water supply, ventilation systems, power supply) typically through adding appropriate additional layers of security
- a process for informing organisers of the different alerts and responses in use onsite so these can be factored into the response plans e.g. different responses are called for in the case of a lockdown versus a general evacuation
- a plan as to how they can support a first response intervention.

Organiser's should review with the venue their assessment of vulnerabilities, control measures and active monitoring in place. Where the event venue is a dry hire, greenfield or where the organiser creates a venue or supporting infrastructure - this assessment may sit solely with the organiser.

Further questions to ask (if necessary) –

- what relationship does the venue have with security intelligence agencies and local authority services
- what measures are in place between events for security sweeps
- what measures are in place for background/ HR vetting of venue staff and 3<sup>rd</sup> party venue contractors
- what links does the venue have with neighbouring businesses/ organisations
- what is the response plan from first response agencies (armed police, fire and emergency care)
- what previous incidents have occurred, what were the outcomes

In many venues there may be a requirement to use approved security suppliers.

Coordination and communication between venue and event security control rooms should be agreed.

Further general security advice can be found in the security section of the [e-guide](#).



### 1.3. Event specific threat review

Organisers must complete a review of the conditional factors based on the event profile, the venue infrastructure and the regional and national security situation to calculate the threat and security risk level. See table below.

The review should demonstrate that the security threats have been considered with steps taken, where practicable, to mitigate. It should be based on the available information and should cover the current threat spectrum.

The mitigation or control measures should be appropriate and proportionate. Focus of control measures should be towards reasonably foreseeable events. For example, an event with military content may require additional entry screening controls to protect against protest. However, a small regional flower show may not.

Where the event specific threat review suggests mitigations that are not selected to be implemented the justifications should be documented.

#### Key principles

- Understanding the terrorist threat and attack methodologies
- Proportionate protective security and preparedness measures
- Importance of vigilance, the reporting of suspicious behaviour
- Plan and prepare for possible terrorist attacks, for example through staff training

#### Sources of security threat information can include:









- [Home Office](#)
- NaCTSO/ [Protect UK](#)
- [NPSA](#)
- [Counter Terrorism Policing](#)
  - o Counter Terrorism Security Coordinator (CT SecCo)
  - o Counter Terrorism Security Advisor (CTSA)
- Police
- Internal security specialists
- External security specialists, for example [PoolRe](#)
- Venue
- Event security supplier
- Event stakeholders – sponsors/ exhibitors/ speakers/ VIPs

The event specific threat review needs to be recorded and retained by venues and organisers and be understood by all key staff. For further information see [Event Communication](#).

A CT SecCO may be assigned to an event by the Police if it is determined necessary. A CT SecCO responsibilities are:

- Identify threat, risk and harm
- Conduct method of attack assessments
- Conduct site or venue visits
- Stakeholder engagement and partnership
- Attend relevant planning meetings
- Provide advice and recommendations on mitigation options and contingencies to policing the event
- Ensure all security activities are conducted legally
- Quality assure measures during the event
- On hand to provide dynamic security advice during the event

The level of a security threat will involve the analysis of the conditional factors, including:

	<b>Factor</b>	<b>Consideration</b>	<b>Potential threat/outcome</b>	<b>Examples</b>
	National/ regional threat levels	Terrorism threat levels Civil unrest Unrelated large mass gathering	Planned protests Unknown/ known events	Festivals Marches Demonstrations Flash mob
	Venue location	Critical National Infrastructure Iconic status/ venue profile Neighbouring businesses/ organisations	Effect on the event if there was an incident locally Invacuation/ lockdown	Public transport hubs Airport Political institutions Social institutions
	Security intelligence	Security consultancy/ supplier e.g. CTSA/ CTPO Local authorities Local Police Venue security Stakeholders	Event industry sector/ venue specific threat Known local threat	Known high level threat Known antisocial behaviour
	Venue preparedness	Infrastructure in place Collocated events at the venue Venue vulnerabilities, such as perimeter security measures, housekeeping, response procedures Access vulnerabilities	Ease of access for hostile actors Exploitation of venue vulnerabilities	
	Industry sector of the event, content areas within the event	Environmental Human rights Animal rights Geopolitical Corporate sensitivities	Sensitive topics can create unwanted interest, additional media coverage and be a target for protest or attack Consideration of VIPs or speakers	Known event sector threat
	Stakeholders involved in the event	Sponsors Exhibitors Visitor profile VIPs, Royalty, Celebrities High profile speakers	Affiliation with contentious parties/ topics	An exhibitor that has a division that works within a contentious area
	Public profile of the event	Media interest Social media coverage Event size Local area prominence	Exposure to cause Increased interest due to stakeholders involved	Live broadcasts
	Previous incidents	Protest Disturbances	Perception of easy access to event Use as a distraction	

The event security assessment and event security measures should always be reviewed if any of the event factors change. This review should be documented/ recorded. Existing planned mitigations may still be very much appropriate.

## 1.4. General Event Security Risk Assessment

A general event security risk assessment should be undertaken in addition to the counter terrorism considerations. This assessment may be part of the overall event risk assessment or also include the [Counter Terrorism Risk Assessment](#) (CTRA).

Risk assessments should demonstrate that the security risks that have been considered with steps taken, where practicable, to mitigate. These risks could include the following:

- 3<sup>rd</sup> Party Security Suppliers (Stand Security)
- Anti-Social Behaviour (assault – verbal/physical/sexual)
- Anti-Social Behaviour (Drugs & Alcohol)
- Anti-Social Behaviour (Venue Location)
- Cash handling
- Crime (High Value Events - Targeted/Professional Crime)
- Crime (opportunistic)
- Crowd Control
- Customer Disputes
- External Events/Late Night Events
- Fraud/Corruption (Fake tickets/ticket touts/Copyright issues)
- Head of State/Government Officials
- Lone working positions (Staff/ Security)
- Lost Children/Vulnerable children/adults
- Protest
- Show Team – Hotel Location/Late Night Events/Welfare
- VIP/Talent

Risks should be identified in conjunction with the Venue, appointed Security Supplier and the Event Commercial Team. Consideration should also be given to any historical information that you have the event including:

- Incident reports
- Police reports
- Event related social media (current and historical)
- Venue Wash Up Reports
- Current Venue Intelligence
- Security Wash Up Reports
- Current Security Intelligence
- Exhibitor/Visitor Complaints
- Exhibitor Profiles (Exhibitor Products)
- Content (Seminars/Conferences)

Activity/ Occurrence	Hazard & Consequences	Who is at Risk	Controls	P	S	Action	Persons Responsible
Anti-Social Behaviour (Alcohol)	Disorientation Violence Slips, trips, falls Irresponsible behaviour leading to minor accidents	Organiser Venue Staff Exhibitor Visitor Temp Staff Security Catering Contractor	Catering staff to be aware of individuals becoming too intoxicated and stop serving them if necessary Challenge 25yrs old policy in place Security to monitor and respond Adherence to venue alcohol policy Ejection Policy in place	1	2	2 - Low	Organiser Venue Catering Manager H&S Manager Floor Manager Security

Security risk assessments should be provided by the venue and/ or the venue security supplier and if different the event security supplier, plus any other stakeholders involved in security activities within the event.

## 1.5. Counter Terrorism Risk Assessment (CTRA)

A Counter Terrorism Risk Assessment (CTRA) provides a record of

- the competent person(s)
- the threats the organisation might face
- who and what might be harmed and how (vulnerability)
- what the company is already doing to reduce or eliminate risk (control measures)
- what further actions are needed to take to get more control of the risk
- who needs to carry it out/ responsible for the control measures
- dates for reviewing progress on the plans and the further actions

Threats that may need to be considered within the CTRA could include

- Hostile reconnaissance
- Bomb threat
- Vehicle as a weapon (VAW)
- Vehicle borne improvised explosive device (VBIED)
- Person borne improvised explosive device (PBIED)
- Marauding terrorist attack (MTA)
- Placed improvised explosive device (IED)
- Fire as a weapon (FAW)
- Chemical, biological or radiological attacks (CBR)
- Unmanned aerial attack (Drone)

Click [here](#) for the link to the ProtectUK template, image shown below



**NATIONAL  
COUNTER TERRORISM  
SECURITY OFFICE**

OFFICIAL



### Risk management template

**Description of site:**

**Responsible person:**

**Competent person(s):**

**Description of process: Date:**

What are the threats?	Possible harm	Controls already in place	Decisions, further actions and responsibilities	Progress Reviews
Who might carry out an attack and what attack methods might they use?	What is the level of risk? Who is vulnerable to the threats (staff, customers, general public, etc.) and are there any with specific vulnerabilities? What harm might be caused and with what consequences?	What defences, plans and other mitigating measures do you already have in place and how effectively will they control terrorist risks?	What further controls are needed and who will take responsibility for ensuring they are implemented?	When will reviews be carried out of the decisions made and of any new or improved controls that have been put in place?

Below is an example of an event specific CTRA

Threat	Vulnerability	Venue Control Measures	Event Control Measures	Additional higher threat level control measures
For all identified threats	<p>High profile event with multiple high-profile stakeholders and media coverage</p> <p>Publicly accessible entrance</p> <p>Multiple access points to the venue – unmanned doors/ sole security position</p>	<p>Venue reaction Standard Operating Procedures (SOPs) in place</p> <p>Venue response (evacuation/ invacuation/ lockdown) SOPs in place</p> <p>Emergency procedures displayed</p> <p>Venue Security Control room where CCTV system is monitored</p> <p>Identified unmanned doors made secured</p> <p>Venue responsible for additional securing of the venue and liaising with police</p> <p>Communication system between venue control room, event security and event organiser operational lead</p> <p>Public address (tannoy) system available for messaging</p> <p>Venue/ event medical/ first aid in place</p>	<p>Event security and relevant event staff briefed on venue security SOPs</p> <p>SOP in place for security and relevant event staff to report unusual activity</p> <p>Emergency procedures issued to exhibitors and contractors pre-show</p> <p>Communication system between event security, event organiser operational lead and the venue control room</p> <p>Public address (tannoy) system available for emergency messaging</p> <p>Event Critical Incident Management Plan in place</p> <p>Key staff to undertake ACT and SCaN training</p> <p>Staff to be briefed in Run, Hide Tell</p>	<p>Exhibition Detection Dog teams patrolling and checking areas of vulnerability</p> <p>Increased frequency of bag checks</p>
Hostile reconnaissance	<p>Event attendance via registration without additional security screening unless there is specific intelligence relating to an individual</p> <p>Prevalence of cameras and phones with photographic capability being used</p> <p>Images of the venue available online (google maps street venue, venue website)</p> <p>Access available regularly by transitional/ temporary event staff</p>	<p>Limited key security/ infrastructure information available online</p> <p>SCaN and other CT training undertaken</p> <p>Venue security trained to recognise unusual behaviour, activities or out of place persons</p> <p>Obvious CCTV cameras and signage</p> <p>HR process for vetting staff and venue appointed contractors</p> <p>Venue security patrols, event traffic staff to manage good housekeeping to ensure external areas are kept clear and regularly patrolled</p> <p>Venue staff identification/ pass system in place</p>	<p>Attendees to the event to issued with an identification badge/ pass</p> <p>SCaN training completed for core operational staff</p> <p>Event security requested to complete SCaN training</p> <p>Event security trained to recognise unusual behaviour, activities or out of place persons</p> <p>Limited floor plan details available online</p> <p>HR process for vetting staff</p> <p>Event security patrols to manage good housekeeping to ensure external areas are kept clear and regularly patrolled</p>	

Counter terrorism risk assessments should be provided by the venue and/ or the venue security supplier and if different the event security supplier.

[Protect UK](#) provides a menu of tactical options or control measures.

In addition, it is expected that preparations are made for the response in the event of an attack. For more information see [4. Response/ Recovery](#).

## 2. Planning

Event organisers need to plan and coordinate with venues to ensure that additional event security measures compliment and support venue arrangements. Additional consideration should be made to other security stakeholders, such as local authorities, law enforcement and third-party event security providers.

Security planning will continually evolve and should be regularly reviewed with a focus on:

- Situational awareness, continual readiness, empirical evidence and up-to-date thinking
- Governance: internal roles, responsibilities, relevant legislation, authorities, accountabilities of security stakeholders and appropriate resourcing
- Appropriate security control measures and operational plans as identified from the event counter terrorism risk assessment and general event security risk assessment
- The cooperation and behaviours of customers
- 

Security and CT planning should not be dependent on policing assets, as even paid for Policing can be redeployed to an incident with little/ no notice. Therefore security plans should be sufficiently evolved and robust enough to not require Policing support.

### 2.1. Vulnerabilities

Throughout the planning process the vulnerabilities that were identified in the assessment stages should be reviewed and considered.

### 2.2. Responsibilities

Detailed plans with clear direction to all staff should be available, with clear delegation of responsibilities relating to control measures and/ or response plans. This should include a review of event spaces, collocated events or businesses and additional surrounding areas (sometimes referred to as last mile, zone x or grey space).

Below is a list of potential tasks/ responsibilities that should be considered and allocated to a particular person or entity. In some cases, responsibility may be shared (for example, within venue shared spaces) or allocated depending on the location (for example, inside/ outside the event halls).

This list is not exhaustive and may have elements which are not relevant.

- Active monitoring security systems
- Control room management (venue/ event)
- Designated protest area
- Emergency procedures/ alarm system
- Employment of security cover
- Evacuation/ lockdown
- Eviction/ Ejection
- External spaces outside of event tenancy perimeter
- Hostile reconnaissance
- Local authority engagement
- Emergency services engagement
- Nomination of a responsible person to cover out of normal hours
- Provide briefing/ training
- Security messaging
- Security of shared/ common spaces outside of event tenancy perimeter
- Response to
  - o Lost child/ vulnerable persons
  - o Lost property
  - o Drone sighting
  - o Chemical incident

Consideration should be given to how responsibilities extend to contractors and other partners on the site (e.g. private contract security providers, catering concession personnel, collocated events). Clear communication of where the expectation of responsibility lies is very important.

## 2.3. Competence

There is a requirement for generic awareness training for staff, with specific identified roles undertaking additional awareness training and exercises to prepare for a potential incident.

Martyn's Law is expected to detail requirements around competency and ProtectUK website/ app will be updated accordingly as more information is available. Please refer to the [ProtectUK](#) for updates as and when they become available.

ProtectUK/ NaCTSO do not endorse any current courses or products that mention supporting either compliance of the Martyn's Law or the Competent Persons Scheme. They are unable, at this stage, to provide any assurance for third party courses that are not endorsed by NaCTSO, or not hosted on the ProtectUK site unless otherwise specified.

A Competent Persons Scheme is currently (Dec 2022) being drafted by the Home Office along with NaCTSO with a time frame of two years to define and roll out the scheme.

### 2.3.1. Training

Details of free training recommended for all relevant personnel and promoted by ProtectUK/ NaCTSO:

Counter Terrorism Policing have created a portfolio of **ACT** (Action Counters Terrorism) training which covers topics such as identifying security vulnerabilities, how to identify and respond to suspicious activity/ items and how to respond to a firearms or weapons attack. Click [here](#) for more information.

See, Check and Notify (**SCaN**) training has 6 modules and covers topics such as vigilance, suspicious activity and reporting, for example relating to hostile reconnaissance. Click [here](#) for more information.

**Run, Hide, Tell** guidance (video and printed) is issued by Counter Terrorism Policing and is for all staff, security and members of the public. There are alternative versions of the advice for a youth audience. Click [here](#) for more information.

Additional training such as **Wave** (Welfare and Vulnerability Engagement) is available and aims to increase the skills, knowledge and confidence of those working in licensed premises focusing on identifying vulnerability and making appropriate interventions. Part of this initiative includes a consumer facing campaign which allows people who feel like they are in an unsafe situation to ask for help using the "Angela" code word, informing a staff member of their need, and allowing them to access discreet help. Wave is based on five key principles:

- Preventing and reducing violent crime linked to the licensed economy
- Preventing and reducing sexual offences
- Reducing preventable injury linked to alcohol and drug use in the licensed economy
- Reducing opportunities for criminal activity and anti-social behaviour in licensed premises
- Promoting partnerships and engagement with communities and key stakeholders in the licensed economy

Click [here](#) for more information.

Event specific training/ briefings should also cover relevant response procedures (e.g. lost child, evacuation/ lockdown, chemical attack, drone sighting, existing venue procedures etc).

### 2.3.2. Licensable activity

The Security Industry Authority ([SIA](#)) is the organisation responsible for regulating the private security industry.

An SIA licence is required to do any of the following:

- screening a person's suitability to enter the event or venue: for example looking out for individuals under the influence of alcohol or drugs or behaving in an anti-social way. This includes those who are searching bags to ensure that there is no unauthorised access or any damage to property or injury to others
- searching people and/or property for the purpose of preventing unauthorised or illegal items from entering the premises e.g. cameras, alcohol, drugs, or weapons
- responding to incidents within crowds, queues, or the audience to control behaviour which is anti-social, undesirable or likely to result in harm to others
- protecting an identifiable area with the intention of preventing unauthorised access or damage
- providing a security presence to prevent and detect crime within a designated area
- guarding property and/or equipment in situ during the set up and breaking down of an event, exhibition or similar
- patrolling the perimeter of an event to prevent unauthorised entry by individuals, whether by climbing or breaching any fences or barriers, or by being let in via an access point
- working as a bodyguard protecting performers, corporate guests, clients VIPs, etc. under a contract for services
- observations and reporting roles as part of, or in support of, guarding. Licensable activity includes providing a physical presence or any form of surveillance to deter or otherwise discourage something from happening, or to provide information if it does happen about what has happened. Examples of such roles include (but are not limited to) patrolling the venue, observing from fixed positions, or monitoring CCTV footage

An SIA licence is not required:

- work as an unpaid volunteer ('unpaid' does not just refer to money: the individual must not receive any reward, benefit, or payment in kind)
- check people have paid for entry to an event or that they have an invitation - but to refuse entry and/or make attendees leave, a licence will be required
- perform stewarding duties, such as directing people to their seats, toilets or first-aid facilities

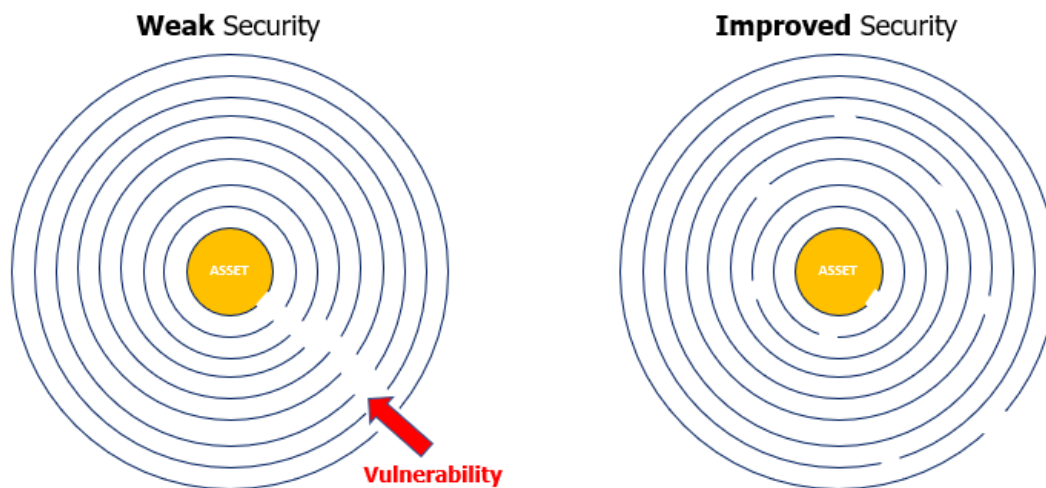
Click [here](#) for more information.



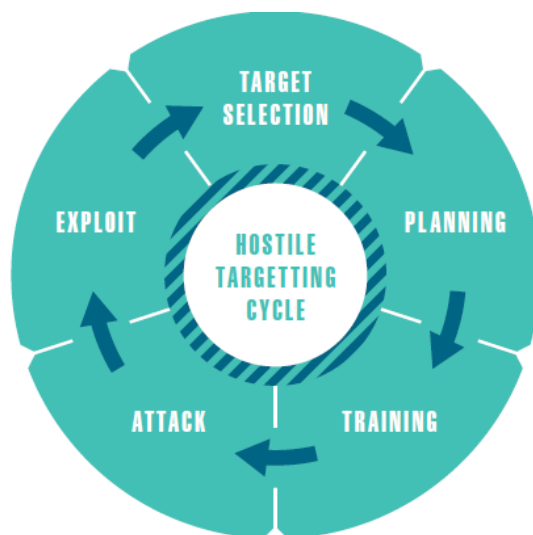
### 3. Control Measures

Effective physical security is achieved by multi-layering different measures. The concept is based on the principle that the security of an asset is not significantly reduced with the loss of any single layer. Each layer of security may be comprised of different elements of interdependent systems.

To achieve success, an adversary will attempt to identify and then exploit any perceived weakness within the protective security measures. Having an effective, proportionate security solution will mitigate the ease with which an adversary can formulate then carry out an attack plan.



Every protective barrier has a weakness – the art is to recognise and manage this vulnerability effectively. Understanding that cycle and how to disrupt it is the key to a successful security policy and planning process.

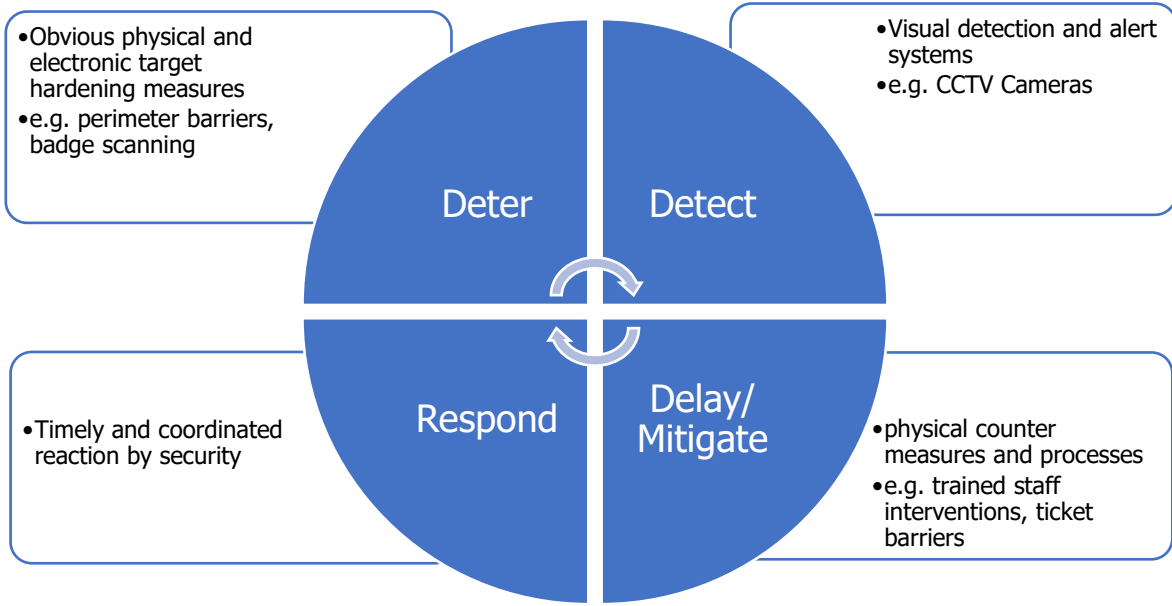


Ref: X-Venture – Public Safety and Security

Security control measures should be reasonably practicable and proportionate to the threat and risk. It is recommended to evaluate whether the measures are:

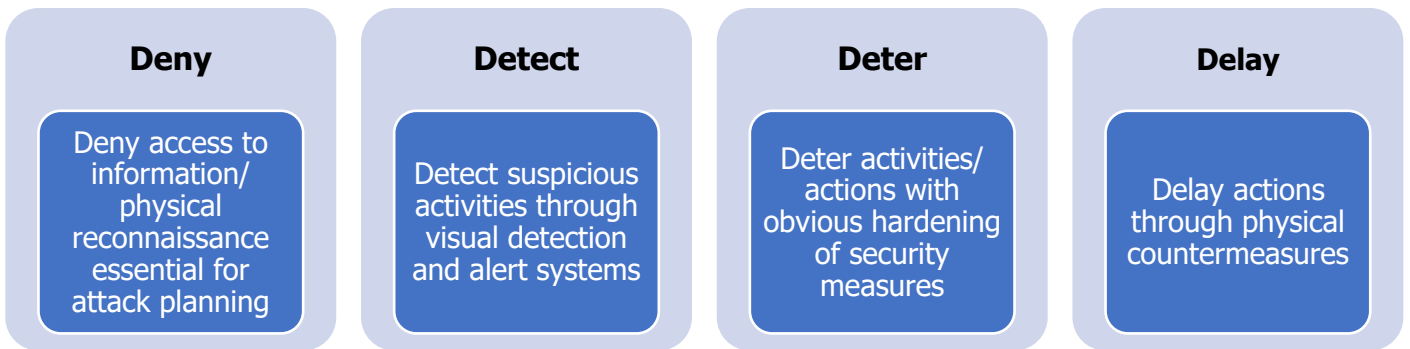
- Justifiable**
- Achievable**
- Sustainable**
- Practical**
- Affordable**
- Reasonable**

### 3.1. Layered Security Measures



Based on [Australia’s Strategy for Protecting Crowded Places from Terrorism](#) (2017) – Layered Security

#### 3.1.1. The 4 Ds



The below table provides examples of possible control measures that could be considered, based on the event specific threat/ security assessment.

<b>What</b>	<b>How</b>	<b>Why</b>
Buildings and infrastructure	CCTV, security control rooms Electronic intruder detection systems Physical barriers, such as hostile vehicle barriers Doors Secure areas Vehicle access Access control	A venue and event with visible security infrastructure will seem a harder target and therefore deter
Perimeter	Fencing indicating demarcation Security fences or environmental barriers including water features/ planters Pedestrian and vehicle access control points Access control measures - Badge/ ticket checking/ scanning Signage/ notices about security measures Vehicle security barriers/ check in system/ exclusion areas/ screening	Efficient perimeter security indicates a proactive approach to security
Search and screening equipment	Bag searches Bag scanners No bag policy Metal detectors, handheld wands Archway metal detectors Canine explosive trace detection (bomb dogs)	Control of entry Stopping contraband Deter and detecting
Security personnel	High visibility security positions and patrols Identifiable Trained and licenced Behaviour detection (Spotters) Security staffing undertaking random patrols within the event Rapid security response team	Visible as a deterrence Identifiable if an attendee needs to report a concern Customer confidence Nonvisible personnel key monitoring tool as a further detection measure Effective response
Front-line staff (non-security)	Vigilance – identifying and challenging Undertake SCaN/ ACT training and briefed to report out of place persons, activities, behaviours	Detect unusual behaviour and potential threats Awareness of vulnerable customers
External resources	Police support/ presence (Project Servitor) Customer service staff ('here to help')	Detect unusual behaviour and potential threats Awareness of vulnerable customers
Customer engagement	Pre event, onsite communications Venue signage, phones, PA system Event signage, security staff Agreed messaging (for PA) Reporting of suspicious behaviour to security officers, event staff	Availability to report concerns or understanding of what to do if there is an incident Create a security conscious environment
Review the information which is publicly available	Detailed floorplans VIP schedules/ movement Images of badges/ passes Changing the design of badge between event editions (if not scanned for verification) Social media	Reduce availability of information to restrict hostile reconnaissance
Staff security awareness	Behaviour outside of the venue/ event (not wearing event name badges) Location of hotels to venue Transport arrangements to/ from hotel/ home Posting security sensitive information on social media	Coercement – knowing/ unknowing Access of information for hostile reconnaissance

### 3.1.2. Scalable Security Control Measures

Example of how a particular security control measure could be scaled to the appropriate security threat level.

Control	Normal	Heightened	Exceptional
Entrance security staff	Suitable and appropriate level of visible/ identifiable trained/ licensed staff	Suitable and appropriate level of visible/ identifiable trained/ licensed staff  Additional support from response teams	Suitable and appropriate level of visible/ identifiable trained/ licensed staff  Additional support from response teams  Additional numbers of staff  Further external perimeter patrols/ monitoring  Additional screening measures  Police support/ presence
Screening — bag inspections	Random visual bag checks	100% visual bag checks	No bag policy  Additional screening such as x ray machines, metal detectors, detection dogs

### 3.2. Vulnerable Groups

If the event involves any vulnerable groups (such as children) a consideration should be made for

- enhanced screening and vetting checks
- visitor management/ access/ egress for customers with restricted mobility
- specific response procedures

Consider vulnerable groups which may have non-visible conditions (e.g. autism) and brief security in any customer service/ support measures that are in place at the event.

There are various schemes to help individuals with hidden disabilities, for example the [Sunflower lanyard](#). It is good customer service to be able recognise and support these organisations.

### 3.3. Special Event Activities

Review security measures needed, if the event involves any special event activities, such as

- VIP/ Celebrity movement/ crowd management
- Royal/ Monarchy Protection
- Visitor participation
- Queuing/ seated theatre/ standing viewing
- Lower lighting/ dark areas/ flashing/ strobe lighting
- Animals
- Live media broadcast

### 3.4. Reporting Suspicious Behaviour/ Occurrences

Staff, particularly those with experience of a venue that know what normal behaviour looks like there, should be empowered and briefed to report anything out of the ordinary. If something or someone does not look right, then something should be done.

An escalation plan is crucial when dealing with suspicious behaviour. Managers should encourage this, and the staff should be made to feel supported when it comes to reporting anything suspicious.

These plans could include dedicated first aid support and should have enhanced first aid kits at key locations and a plan around casualty handling.

Key to the success of emergency response is as follows:

- Assessment of risks of threat to life that account for the risk profile of the venue and the event
- Close liaison and cooperation between the event organiser and the venue where these are separate parties
- Clear protocol on who takes control in the event of a life-threatening emergency (normally the venue)
- Clear, unambiguous emergency procedures that are understood by all
- Mechanism for stand down in the event of a false alarm

### **3.5. Event Communication**

There are a variety of considerations regarding a general communications strategy for events and the below information is not exhaustive due to the range, size, scope and location of events. As part of a general communications strategy, relevant information on security/ safety measures, plans (access/ egress control), escalation processes and key personnel should be included.

Key personnel may include a range of stakeholders including:

- Venue
- Local authority and agencies
- Exhibitors
- Contractors
- Suppliers
- Event organiser team
- Staff
- Security team
- Temporary event staff
- Visitors

Consider how best, and when, to communicate relevant security information to each stakeholder. Further consideration should be made to the demographic of the audience when deciding on the communication method.

A common method to ensure all parties are given updated information at the same time is via a dedicated 'security briefing'. These briefings can be conducted before, during and post incident (also known as a 'hot debrief').

The security briefing is an opportunity to communicate a range of important aspects which could include, but not limited to:

- Key roles & responsibilities of management/ staff
- Known risks and mitigation plans
- Methods of communication (radios/ phones) and escalation process
- Emergency plans

Coordination and communication between venue and event security control rooms should be agreed.

#### **3.5.1. Security Minded Communications (SMC)/ Deterrence Communications**

It is important to ensure guests/ visitors and delegates are also provided with relevant security information prior to arrival and during the event. This could include conditions of entry, such as prohibited items, registration/ badging requirements and positive security messaging including CCTV usage and reporting processes.

There will be some sensitive security information that you will want to protect and not share openly. This information could include:

- Specific security procedures
- Detailed floor plans (locations of storage areas, VIP rooms, cash offices etc)
- Detailed VIP schedules
- Copies of passes/ badges which could be replicated

External communications, such as the event website or visitor emails can be used to promote the security measures that will be in place and act as a deterrent to potential hostiles. It is often the most cost effective control measure.

When creating content, consider:

- What needs to be communicated?
- How can this opportunity be used to include messaging that could deter a hostile?
- How can information be provided without giving away details that would be potentially useful to a hostile?
- If detailed information needs to be published, how can any vulnerability be countered by promoting the protective security measures in place?

Protect UK have provided various vigilance campaign for national events and activities and advise that the public understand that vigilance messaging is there to keep them safe, that they don't feel alarmed when they see counter terrorism messaging, but they are reassured and informed on how to report suspicious activity.



The National Protective Security Authority (NPSA, formerly known as CPNI) have provided [further guidance](#).

## 4. Response and Recovery

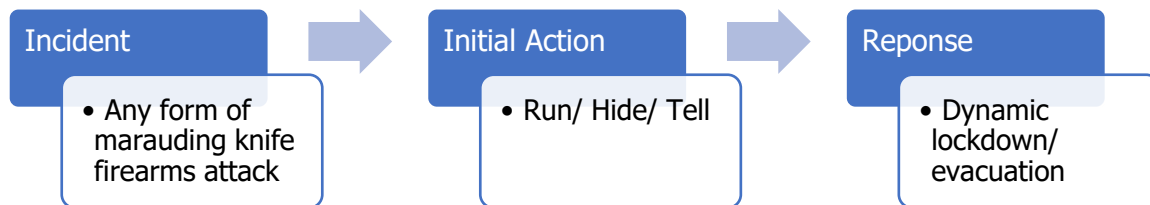
Responding to a security threat occurrence requires a timely and coordinated security response throughout a venue or event area of control. Prior to going onsite for the event a clear plan of actions and responsibilities should be established with the venue, the security supplier(s) and external agencies (e.g. police).

These plans must be communicated to all relevant parties, with clear allocation of responsibilities relating to response plans.

Important elements of response include:

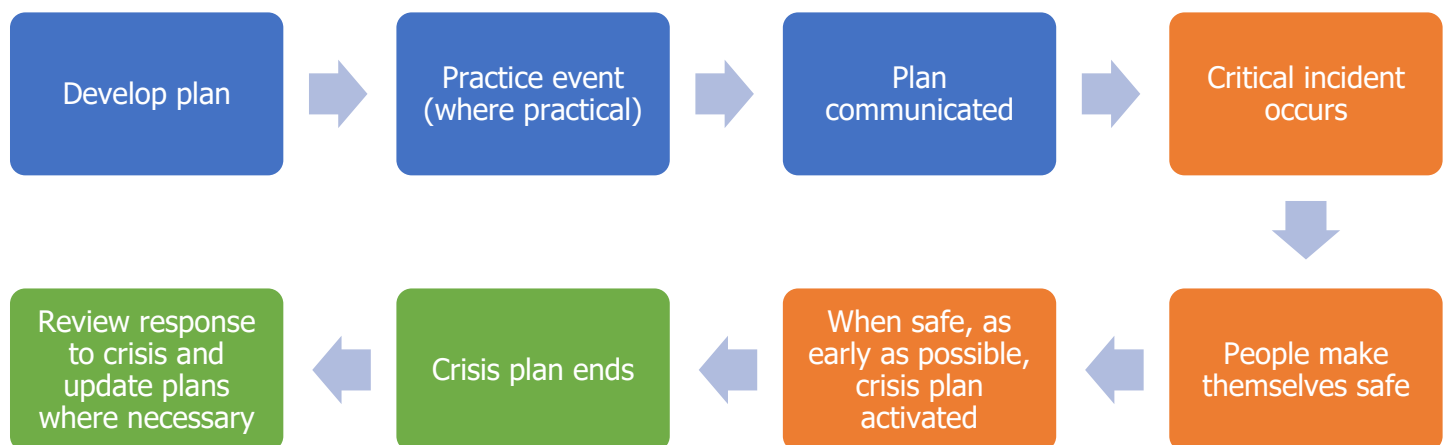
- Security staff who can **respond effectively**, possess the requisite **training** and **competence** and have access to appropriate **equipment** (e.g. first aid kit) to deal with or limit the impact of an incident
- **Clear allocated roles and responsibilities** between all relevant parties, particularly when there are multiple events within the same venue and/ or event security working alongside venue security
- Reliable **emergency communication systems** between all relevant parties
- Comprehensive **security plans** that are understood by all staff and security personnel, regularly exercised, and in line with local emergency services plans.

Make considerations for a variety of situations, understanding that the situation will often result in a limited number of resulting actions, for example, evacuation, invacuation or lockdown.



The safety of all individuals, whether they are staff, security or customers, should always be made a priority in any response. The current guidance for most scenarios is Run, Hide, Tell -click [here](#).

### 4.1. Critical Incident Management Plan



For further guidance from HSE on Planning for incidents and emergencies click [here](#).

## 4.2. Procedures

There are various sources available for guidance and advice on actions and examples, below are a selection

### 4.2.1. Evacuation/ Invacuation/ Lockdown

There are a number of options for emergency response, including:

- full site evacuation
- phased evacuation
- partial or zonal evacuation
- directional evacuation, in which staff, contractors and visitors are directed to specific exits and routes
- invacuation to safer areas, including protected space(s), if available
- partial invacuation
- no action required (a decision is made not to evacuate or invacuate)
- lockdown (this may be a partial or full lockdown)

Any emergency response should include suitable provision for individuals at an event who might have additional needs, for example mobility restrictions. The emergency response decision would normally be agreed with the venue and event security, and if applicable, coordinated by venue security.

### 4.2.2. Protest plans

If during the assessment process it is identified that the event has a vulnerability to a protest, planning and response procedures should be considered.

The type of protest and protestor will need to be reflected in the response plans. Looking at prior protest activities can provide useful intelligence on possible actions taken.

Considerations could include:

- security response team
- ejection/ eviction process
- protest 'pen'/ area
- scale of protest
- social media monitoring

Event organisers, venue security and event security should be mindful that protest activities can be used as a distraction technique. Protest activities may also escalate in size and action so it is recommended to maintain continual monitoring and review of the situation.

In the situation of collocated events the impact of any potential protest activity should be reviewed and discussed with the venue and event security teams(s).

### 4.2.3. Other Threats

[Protect UK](#) has various resources covering response guidance for the below specific threats -

- Attack methodology: Improvised Explosive Devices (IEDs)
- Attack methodology: Vehicle bombs
- Unattended and suspicious items
- Bomb threats
- Chemical, Biological and Radiological (CBR) attacks
- Marauding Terrorist Attack (MTA): RUN HIDE TELL
- Countering threats from Unmanned Aerial Systems (C-UAS)
- Vehicle as a weapon



#### 4.2.4. Communication Plan

The venue and event should have a predetermined detailed communications plan to be used in the event of a crisis. If the event is in a dry hire venue, greenfield or similar, then the responsibility of the communications plan may fall solely on the event organiser.

A communication plan may include (please note that this list is not exhaustive):

- Escalation process
- Event team contact details
- Company management contact details
- Out of hours/ duty manager details
- Back up team considerations
- Venue and security stakeholder contact details
- Alternative methods of communication

#### 4.2.5. DIM ALICED

Using the 'DIM ALICED' principle for crowd management a communication plan in the case of an emergency situation can be created. By reviewing design limitations (such as capacity, flow rates), communication of information (social media, signage, PA announcements, external parties such as news outlets) and management systems (processes and procedures for example, venue emergency procedures), a plan of how to effectively communicate and influence crowd behaviour. Requirements for vulnerable groups involved in the event should also be considered as part of this process.

	<b>Design</b>	<b>Information</b>	<b>Management</b>
<b>Arrival</b>	How visitors would be travelling to the event	Venue travel and parking details on show website	Liaising with local transport provider
<b>Last Mile</b>	Flow of visitors from transport to event perimeter	Directional signage	Car park traffic management
<b>Ingress</b>	Space and process of entry – checking tickets/ badges, bag searches, cloakroom Queuing systems Welfare facilities	Staffing (stewards) to manage queueing SIA security at entry points	Queuing layouts Additional staff for cloakroom
<b>Circulation</b>	Review areas within the event which will create crowds to gather Review 'bottle neck' areas within the event	Staffing (stewards) to manage flow Signage Scheduling of theatre sessions	Floorplan layout design
<b>Egress</b>	Emergency exit routes Visitor flow at the end of the event	Event timings published PA announcements Stewards to manage flow	Scheduling of theatre sessions to stagger finishes Additional staff for cloakroom
<b>Dispersal</b>	Public transport options Car park exit capacities	Venue travel and parking details on show website	Liaising with local transport provider Car park traffic management

To review alternative methods of communications depending on demographic a matrix system could be used. A template example can be found below

<b>Age/ Type</b>	<b>Local</b>	<b>National</b>	<b>Social</b>	<b>Signage</b>	<b>Email</b>	<b>Phone</b>	<b>Stewarding</b>
<b>0-10</b>							
<b>10-14</b>							
<b>14-18</b>							
<b>18-25</b>							
<b>25-35</b>							
<b>35-45</b>							
<b>45-60</b>							
<b>60+</b>							

<b>Key</b>
Not affective
Partially effective
Effective

#### 4.2.6. Communication Hierarchy

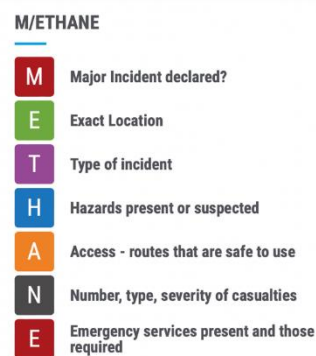
Often Incident Management Plans mirror the command structures used by the emergency services – Gold, Silver, Bronze. Gold is seen as strategic or directing, Silver as tactical or coordinating and Bronze is operational or the doing team. These roles may cover various functions within the event team.

For more information about the police GSB structure click [here](#).

#### 4.2.7. METHANE

The M/ETHANE model is an established reporting framework which provides a common structure for responders and their control rooms to share incident information which could also be applied to an event situation.

For more information on the M/ETHANE model from the JESIP website please click [here](#).



#### 4.2.8. Medical Response

The organiser should ensure that appropriate levels of medical provision is in place based on the event requirements/risk assessments. Where required, additional professional advice may need to be sought. Specific medical provision may be prescribed by any Safety Advisory Group (SAG) involvement in the event planning.

For guidance on specific counter terrorism first aid (ProtectUK) – click [here](#). And for further information about Trauma Kits – click [here](#)

#### 4.2.9. Decision Log

It is important to document decisions and consideration should be made to the method of how this is done. The role of documenting decisions (often called a scribe) should be allocated to a predetermined individual and the experience and competence of this person should be considered.

### 4.3. Response Communication

Communicating effectively during a critical incident is an important element of a successful response plan.

Often there is a need for separate internal and external communication. Understanding how, when and who is responsible for this should be allocated within the [communication hierarchy](#).

#### 4.3.1. Internal

Immediate considerations should be made to accounting for staff and event employees. Multiple methods of communication may be required to provide any updates of information, particularly during an active situation, for example radios, mobile phones and messaging platforms. Depending on the event specific requirements organisers may wish to explore specialist emergency response applications.

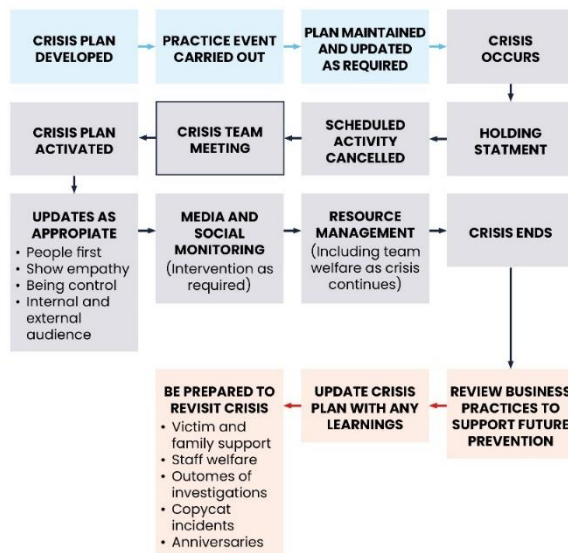
#### 4.3.2. External

When communicating externally a consideration should be made on whether a holding statement is required prior to more detailed information is provided. The agreement process of any external statements should be predetermined and described in the [critical incident management plan](#).

External stakeholders may include:

- Venue
- Local authority and agencies
- Exhibitors, sponsors and other commercial event partners
- Contractors and suppliers
- Security team
- Visitors, guests (e.g. VIPs), speakers and other event attendees
- Media
- Collocated events and neighbouring businesses that may be affected

Please click [here](#) for Protect UK guidance relating to crisis management for terrorist related events for marketing, communication and PR professionals.



#### 4.3.3. Announcements

If the event is responsible for making PA announcements advice from ProtectUK is that they should be:

- Authoritative
- Concise
- Specific
- Repeated
- Frequent
- Reassuring

Click [here](#) for more information. Prepared templates may be included in the event [critical incident management plan](#).

## **4.4. Review**

The necessity for review is divided into 2 main requirements:

- 1) Regular procedural review
- 2) Post incident review

It is recommended that event organisers be well prepared in advance for both as understanding the information you need to conduct each type of review makes it less likely that key information and learning points will go unrecorded.

### **4.4.1. Regular Procedural Review**

This is a key part of the Assessment process covered earlier in this guidance. A review of integral elements of security planning should be regularly scheduled as a part of the Assessment process and further evaluations conducted should a triggering event occur.

Examples of such triggers include but are not limited to:

- A change in the National Threat Level
- A notable security incident occurrence (national/ international) which does not change the national threat level but impacts the event profile or events industry
- A material change in the event set-up or operations, such as a venue change
- Inclusion of a new element or stake holder with unassessed security implications, such as a new event collocated at the venue, high profile exhibitor or media driven interest

### **4.4.2. Training/Briefing**

Regular procedural review should also encompass training and briefing of staff to ensure that:

- 1) Any modifications to the procedures are communicated to staff
- 2) New employees are made aware of their responsibilities and duties

Consideration should be given to the form training takes:

- Briefings
- Tabletop exercises
- Practice drills
- Online courses

All the above are potentially useful and it may be useful to share any significant outputs from training sessions with external stakeholders to make sure the response to incidents is synchronised and effective.

Further details of recommended training can be found in the [Planning](#) section of this document.

### **4.4.3. Record Keeping**

It is important to record these standard reviews and training sessions so that it is clear:

- what processes are in effect
- when reviews are due
- who has been trained

### **4.4.4. Review Points**

As a part of standard post-event review event organisers should consider if the controls in place continue to be appropriate, proportionate and effective for the next iteration of the event. Examples of the recommended standard review points are included below but these are not exhaustive:

- An audit of the registration process, including the design/ branding of badges/ tickets which should be updated regularly to help prevent misuse of old tickets
- Consider any new technology or systems that might provide additional layers of security measures
- Learning points from the last event - what were the weaknesses, strengths and innovations. How should these be reflected in the procedures for the next event
- Feedback from internal/ external stakeholders
- Review of incidents and reports, see below

#### **4.4.5. Post Incident Review**

Should an incident occur during an event it is important to conduct a review of the incident and the response as soon as practically possible.

To ensure the review process is as productive as possible it is important to gather all the appropriate resources/ information and to conduct the review as soon as is practically possible. Consider the following:

- Incident timeline – what was the sequence of events?
- Reports from other stakeholders such as venue or security supplier and, if involved, any emergency services
- Any primary information such as witness accounts, report logs, CCTV/ social media footage and emails from the time of the incident
- Impact reports – who was affected, how? Any casualties/ injuries? Medical reports? Property damage, reputational exposure, welfare requirements?
- Current processes – match your response against your pre-event process to identify what went according to plan and where additional steps were needed

The main focus of this process is to:

- Understand the detail and study the incident to look for improvements
- Identify the vulnerabilities and adapt the planning/ processes of the event to reduce the risk of the incident recurring
- Document findings and any updates to procedures
- Put in place necessary welfare provisions for staff, temporary staff, security supplier or any other stakeholders
- Communicate and reaffirm any updates in relevant processes and procedures
- Ensure any lessons learned are incorporated into the processes for the event

#### **4.4.6. Wellbeing**

Internal post-event reviews are an opportunity to learn, take responsibility and focus on achievable outcomes, they are not an opportunity to assign blame.

Particularly in the case of serious incidents where staff have been exposed to stress, risk or danger it is important that your review processes take into account the wellbeing of those involved and where necessary take advice on what additional support should be offered to those involved.

#### **4.4.7. Conclusions**

When you have drawn and documented the conclusions and identified improvements make sure that you assign ownership and tasks to make sure that necessary changes are implemented.

# Appendixes

[Appendix 1 – Acronyms](#)

[Appendix 2 – The Risk Management Process](#)

[Appendix 3 – The Risk Management Model](#)

[Appendix 4 – National Decision Model](#)

## Appendix 1 - Acronyms

AACS	Automatic Access Control Systems
ABC	Accurate, brief and clear
ADS	Active delay systems
AED	Automated external defibrillator
ACT	Action Counters Terrorism
ALM	Al Muhajiroun
ANPR	Automatic Number Plate Recognition
AQ	Al-Qa-ida
BAU	Business as usual
BBFW	Bladed or Blunt Force Weapon
BCM	Business Continuity Management/ Manager
BDO	Behavioural detection officer
BNP	British National Party
BR	Business recovery
BTP	British Transport Police
C&C	Command and control
CBR	Chemical, biological or radiological
CCTV	Close circuit TV
CIRA	Continuity Irish Republican Army
CM	Crisis management
CNI	Critical national infrastructure
COTS	Commercial off the shelf
CP	Close protection
CPIW	Competent Person in the Workplace
CPS	Competent Persons Scheme
CPNI	Centre for the Protection of National Infrastructure (now known as NPSA)
CPS	Competent Persons Scheme
CSO	Chief Security Officer
CTBIE	Counter Terrorism Business Info Exchange
CTPO	Counter Terrorism Protection Office
CTSA	Counter Terrorism Security Advisor
CT SecCO	Counter Terrorism Security Coordinator
CTSSR	Counter Terrorism Security Specialists Register
DBS	Disclosure and Barring Service
DMD	Discriminative metal detection system(s)
DR	Dissident republican (NI)
DTI	Detect, Track and Identify
EDD	Explosive Detection Dogs
EDL	English Defence League
ERP	Emergency Response Plan
ERT	Emergency Response Team
ERWT	Extreme right-wing terrorism
ETHANE	Exact Location Type of incident Hazards present or suspected Access - routes that are safe to use Number, type, severity of casualties Emergency services present and those required
FAW/ FAAW	Fire as a weapon
FCDO	Foreign Commonwealth and Development Office
FOI	Freedom of information
FPP	Final preparation points
FREC	First Response Emergency Care

FRS	Fire and Rescue Services
FRZ	Flight restriction zone
FTAC	Fixated Threat Assessment Centre
GDS	Gunshot detection system
GSB	Gold/ Silver/ Bronze
HSA	Hostile State Actors
HSG	Homeland Security Group
HME	Homemade explosives
HO	Home Office
HOT	Hidden/ Obvious/ Typical
HVM	Hostile vehicle mitigation
IE	Information exchange
IED	Improvised explosive device
IRA	Irish Republican Army
IM	Incident management
Incels	Involuntary celibates
IR	Incident response
ISIL	Islamic State of Iraq and the Levant
ISR	Intelligence, surveillance, reconnaissance
ISTAR	Intelligence, surveillance, target acquisition and reconnaissance
JDM	Joint decision model
JESIP	Joint emergency services inoperability principles
JOP	Joint Operating Principles
JSO	Just Stop Oil
JTAC	Joint Terrorism Analysis Centre
LASIT	Left-wing, Anarchist and Single-issue terrorism
MMS	Ministry of State Security
MTA	Marauding terrorist attack
MTFA	Marauding terrorist firearms attack
NA	National Action
NaCTSO	National Counter Terrorism Security Office
NCA	National Crime Agency
NCSC	National Cyber Security Centre
NCTAS	National Canine Training and Accreditation Scheme
NF	National Front
NILO	National Inter-Agency Liaison Officer
NIRT	Northern Ireland-related Terrorism
NPoCC	National Police Coordination Centre
NPSA	National Protective Security Authority
NSRA	National security risk assessment
OR	Operations requirement(s)
OSCT	Office for Security and Counter Terrorism
PA	Public Address
PA	Patriotic Alternative
PAL	Publicly Accessible Location
PBIED	Person borne improvised explosive device
PB	Petrol bomb
PDCA	Plan, Do, Check, Act
PIDS	Perimeter Intrusion Detection System
PSC	Private security contractor
PSeMS	Protective Security Management Systems
PSIA	Protective Security Improvement Activity
RAR	Recognise, assess, react
RHT	Run Hide Tell



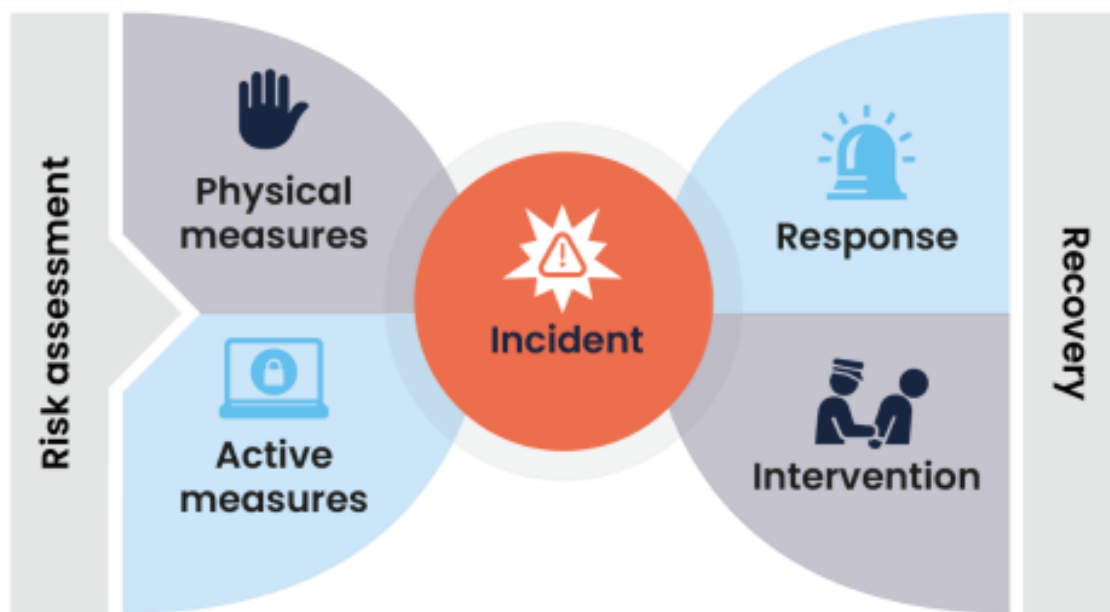
RPG	Rocket Propelled Grenade
RWE	Right wing extremist
RWT	Right wing terrorism
SAG	Safety Advisory Group
SASS	Site assessment security system
SCA	Security considerations assessment
SCG	Strategic coordinating group
SCR	Security control room
SCaN	See Check and Notify
SECO	Police security coordinator
SeMS	Security Management System
SHAC	Stop Huntingdon Animal Cruelty
S-IT	Self-initiated Terrorism
SMC	Security minded communications
SOC	Serious and Organised Criminals
SOP	Standard operating procedures
TTP	Tactics, techniques and procedures
TIC	Toxic industrial chemicals
TTX	Tabletop Exercise
TVRA	Threat, vulnerability risk assessment
UAS	Unmanned aerial system
UAV	Unmanned aerial vehicle (drone)
VA	Vulnerability Assessment
VAW/ VAAW	Vehicle as a Weapon
VAWG	Violence against women and girls
VACP	Vehicle access control point
VBIED	Vehicle borne improvised explosive device
VSB	Vehicle security barrier
VTS	Vertical transport systems (e.g. lifts, escalators)
WHAT	What/ How/ Alone/ Threat

## Appendix 2 - The Risk Management Process



Ref: Protect UK

### Appendix 3 - The Risk Management Model



Ref: Protect UK

## Appendix 4 - National Decision Model

The workflow within the guidance is based on the National Decision Model utilised by Police and other government agencies around planning. Click [here](#) for latest version.



Ref: [National decision model | College of Policing](#)

## Disclaimer

The AEV, AEO and ESSA trade associations are managed by the EIA secretariat. EIA advocates that members of all three associations work within or beyond the requirements of UK law. Where Protect UK, NaCTSO, NPSA, HSE guidance, approved code of practice, other central or local government guidance or examples of case law suggest that specific working methods or standards are needed to meet the requirements of UK law, the EIA advocates that members adopt these.

In instances where groups of members wish to collaborate on finding alternative, but equally as safe, methods of work that they feel are more suited to the operational constraints of the event industry than those described elsewhere, the EIA will facilitate that collaboration and any benchmarking or HAZOP activity that is required, advise members of their specific duties and liabilities and where requested publish their findings.

The EIA cannot and does not however officially advocate any standard or working practice other than those produced by Protect UK, NaCTSO, NPSA, HSE or other government agencies and offices, whether published within the guidance or not, and reminds all organisations, members and non-members alike, that it is their individual responsibility to assess the risks of their work and to establish practices that comply with the law.