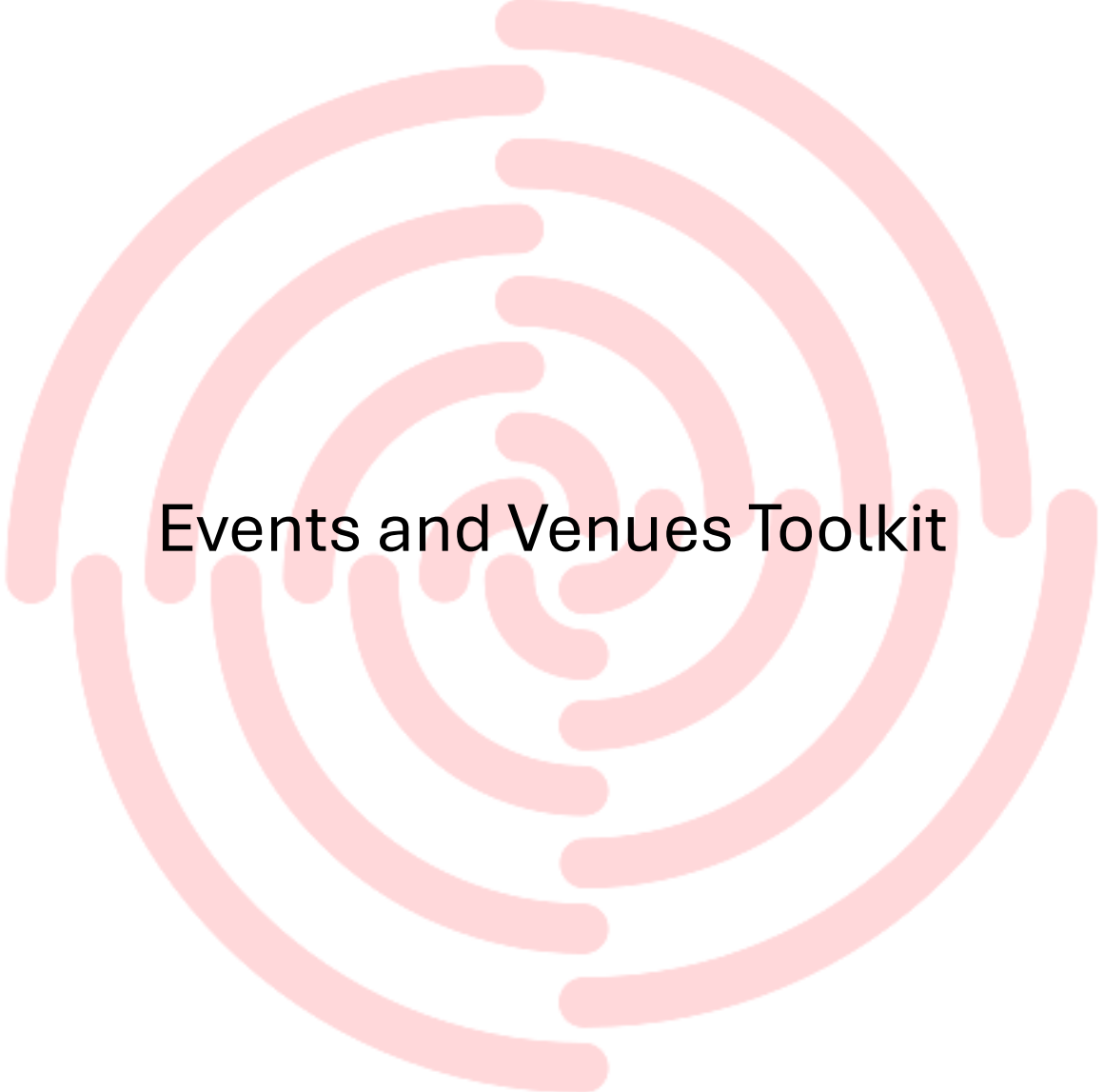




Events and Venues Toolkit

Table of Contents

<i>Executive Summary</i>	<i>4</i>
<i>Background and Context</i>	<i>6</i>
<i>Toolkit Scope and Structure</i>	<i>6</i>
<i>Application and Benefits.....</i>	<i>9</i>
<i>PART 1: Leadership & The Responsible Person</i>	<i>11</i>
<i>PART 2 - People, Training and Readiness</i>	<i>14</i>
<i>PART 3 - Working with Others</i>	<i>18</i>
<i>PART 4 - Understanding Risk</i>	<i>21</i>
<i>PART 5 - Protective Measures and Public Protection.....</i>	<i>26</i>
People: Awareness and Engagement	27
Processes: Clear and Practical Procedures	27
Physical and Technical Measures	28
<i>PART 6 - Operating Within the Wider Framework.....</i>	<i>30</i>
<i>PART 7 - Readiness and Assurance Checklist</i>	<i>32</i>
Before an Event / Operation	32
During an Event / Operation.....	33
After an Event / Incident	34
<i>PART 8 - Validation of Process</i>	<i>34</i>
<i>PART 9 - Readiness, Exercising and Capability.....</i>	<i>37</i>
Exercising Approaches	39
Session Feedback and Evaluation	46
<i>PART 10 - Business Continuity Planning.....</i>	<i>47</i>
<i>PART 11 - Incident Response and Recovery.....</i>	<i>50</i>
<i>PART 12 - Collaboration and Coordination Tools</i>	<i>54</i>
Shared Situational Awareness	54
Purpose of a Communication Plan	59
Radio Communication	65
<i>PART 13 - Technical and Physical Security.....</i>	<i>67</i>
1. Security Equipment and Maintenance	67
2. Technology Integration Resources	67
3. Physical Security Measures	68
4. Crowd Management Tools	68
5. Access Control	68
6. Communication Tools.....	68
7. Cost-Effective Measures for Grassroots Organisations	69
8. Additional Resources.....	69
<i>PART 14 - Hostile Vehicle Mitigation (HVM) and Traffic Management.....</i>	<i>69</i>
Why HVM Matters.....	70
Simple Measures to Deter and Defend Against Vehicle Attacks:	71
Considerations for Grassroots and Smaller Organisations.....	72
Hostile Vehicle Mitigation and Anti-Terrorism Traffic Regulation Order (ATTROs) – Understanding the Legal and Operational Context	72

<i>PART 15 - Other important considerations</i>	74
Emergency Traffic Regulation Notices	74
Section 14 Public Order Act 1986	75
Civil Contingencies Act 2004 – Emergency Powers	75
Planning Conditions and Licensing Restrictions	75
Designated Protection Zones (DPZ) (upcoming and subject to further guidance)	76
<i>PART 16 - Policies and Documents</i>	76
1. Readiness Review	76
2. Public Protection Procedures	77
3. Risk Assessment Record	77
4. Training and Competency Records	78
5. Generic Checklists for each phase of the event	78
6. Incident Reporting Template	82
7. Staff Briefing Checklist	83
8. Suspicious Item Reporting Form	85
9. GDPR Compliance Guidance	87
10. Document Storage and Sharing Guidelines	87
11. Annual Review	87
12. Optional: Public-Facing Policies	87
<i>PART 17 - Directors and Officers Insurance: Protecting Decision-Makers</i>	88
Why D&O Insurance Is Relevant	88
Key Features of D&O Insurance	88
How to Include D&O Insurance in Compliance Planning	89
<i>PART 18 - Primacy</i>	90
What Is Primacy?	90
What to Do When Primacy Is Transferred	90
Actions While the Police or Government Agency Has Control	91
What to Do When Control Is Handed Back	91
Key Considerations	92
Supporting Tools	92
<i>PART 19 - The legal bit: Decision Support Centre (DSC) & National Events Database (NED) Disclaimers</i>	92
1. General Disclaimer	93
2. Limitation of Liability	93
3. No Guarantee of Outcomes	94
4. User Responsibility	94
5. Third-Party Links or References	94
6. Intellectual Property Disclaimer	94
7. Compliance with Regulations	94
8. Tailored Solutions Disclaimer	94
<i>Appendices:</i>	96
APPENDIX A - MEMORANDUM OF UNDERSTANDING	97
APPENDIX B – TRANSFER OF PRIMACY TO POLICE OR GOVERNMENT AGENCY – DOC 1 of 2	99
APPENDIX C - TRANSFER OF PRIMACY FROM POLICE OR GOVERNMENT AGENCY – DOC 2 of 2	101
APPENDIX D - Information Sharing Agreement (ISA) Template	102
APPENDIX E – DSC Readiness Review Template	105
APPENDIX F - DSC Validation of Process (VoP) Workshop Template	107
APPENDIX G - DSC Safety Advisory Group Guidance (SAG / ESAG)	110

* Correct at time of publication

Executive Summary

Events and venues operate in dynamic, often unpredictable environments.

They bring people together in ways that are valuable, but which also require careful thought, coordination and preparedness. Risks are rarely confined to a single site or moment in time. They are shaped by people, place, timing and the wider environment in which activity takes place.

This Toolkit has been developed to support organisations in navigating that reality.

It is not a compliance manual, and it is not intended to replace existing guidance or regulatory frameworks. Instead, it provides a practical, structured approach to understanding risk, making informed decisions and operating with confidence in real-world conditions.

While it aligns with the intent of the Terrorism (Protection of Premises) Act 2025 (Martyn's Law), its purpose is broader. It focuses on how preparedness is applied in practice - before, during and after an event or period of operation.

A Practical Approach to Preparedness

The Toolkit is built around a simple principle:

Preparedness is not defined by what is written in a plan, but by how effectively organisations can respond, adapt and recover when it matters.

It supports organisations to:

- understand risk in context, including factors beyond the immediate site
- apply proportionate and practical measures
- coordinate effectively with partners and stakeholders
- communicate clearly and consistently
- respond to incidents with confidence
- and learn from experience to strengthen future readiness

Designed for Real-World Use

This is a working resource. It is intended to be used flexibly, allowing organisations to focus on what is most relevant to their environment, scale and level of experience.

It has been designed to support:

- grassroots and community-led events

- independent venues
- local authorities
- and large-scale or complex operations

There is no single “correct” way to apply it. Its value lies in how it is adapted and embedded within each organisation’s operational reality.

Leadership, Coordination and Shared Responsibility

At the heart of the Toolkit is the recognition that:

Responsibility may sit in one place, but effective outcomes depend on how well people, teams and organisations work together.

The Responsible Person plays a central role in this, but preparedness is not delivered by individuals alone. It depends on:

- clear roles and responsibilities
- effective communication
- shared situational awareness
- and strong relationships with partners

From Planning to Readiness

Planning is important, but it is only one part of preparedness.

This Toolkit places equal emphasis on:

- people and capability
- validation of process (BAU)
- readiness and exercising
- and continuous improvement

It reflects the reality that organisations must be able not only to plan, but to operate, adapt and make decisions in real time.

A Living Approach

Guidance, expectations and operating environments continue to evolve.

This Toolkit should be seen as part of an ongoing process - one that is:

- reviewed
- tested
- and refined over time

Preparedness is not a fixed state. It is something that is built and strengthened through use, experience and learning.

Background and Context

The Decision Support Centre (DSC) Toolkit has been developed to support venues, events and organisations in preparing for, responding to and recovering from a wide range of safety and security challenges.

It is designed as a practical, working resource, not just a reference document, helping teams understand risk, make informed decisions and operate with confidence in real-world environments.

While it aligns with the expectations of the Terrorism (Protection of Premises) Act 2025 (Martyn's Law), the Toolkit is not built around compliance alone. Instead, it focuses on how preparedness is applied in practice, across different types of venues, events and operating contexts.

Events and venues are rarely self-contained. They operate within wider environments shaped by people, place, timing and external influences. Risks do not begin or end at the site boundary, and effective preparation depends on how well organisations understand and coordinate with that wider picture.

This Toolkit reflects that reality.

It provides proportionate, scalable guidance that can be adapted by:

-  grassroots and community-led events
-  independent venues
-  local authorities
-  large-scale and complex operations

At its core, the Toolkit supports a simple but critical objective:

To help organisations be ready - not just to plan, but to respond, adapt and recover when it matters.

Toolkit Scope and Structure

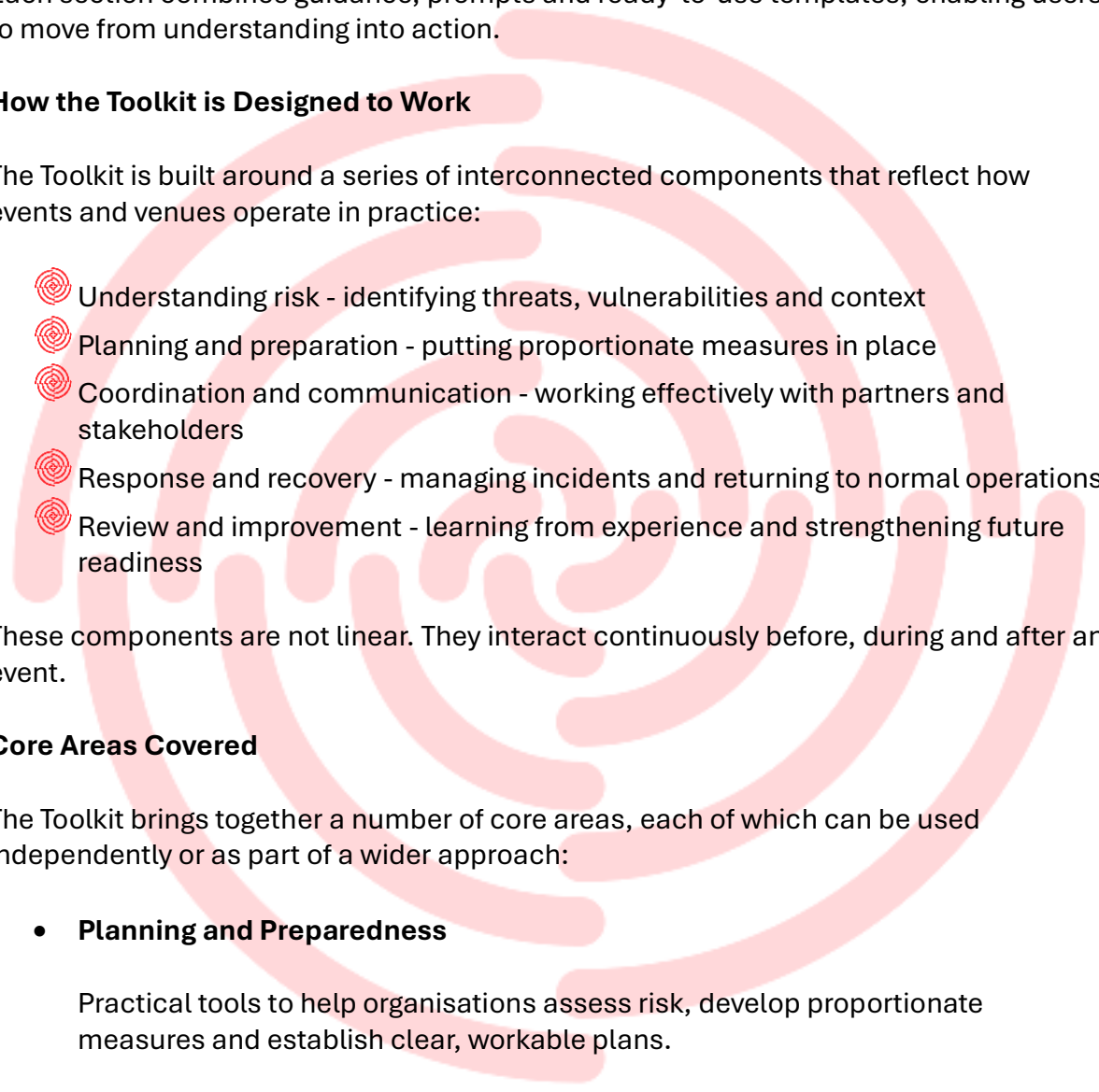
The DSC Toolkit is structured as a modular, practical resource designed to support real-world planning, delivery and response across venues and events of all types and scales.

Rather than being read cover-to-cover, it is intended to be used flexibly, allowing organisations to focus on the areas most relevant to their environment, level of experience and risk profile.

Each section combines guidance, prompts and ready-to-use templates, enabling users to move from understanding into action.

How the Toolkit is Designed to Work

The Toolkit is built around a series of interconnected components that reflect how events and venues operate in practice:

- 
-  Understanding risk - identifying threats, vulnerabilities and context
 -  Planning and preparation - putting proportionate measures in place
 -  Coordination and communication - working effectively with partners and stakeholders
 -  Response and recovery - managing incidents and returning to normal operations
 -  Review and improvement - learning from experience and strengthening future readiness

These components are not linear. They interact continuously before, during and after an event.

Core Areas Covered

The Toolkit brings together a number of core areas, each of which can be used independently or as part of a wider approach:

- **Planning and Preparedness**

Practical tools to help organisations assess risk, develop proportionate measures and establish clear, workable plans.

- **Leadership and Accountability**

Guidance on the Responsible Person role and how responsibility is understood, applied and coordinated across teams and partner organisations.

- **People and Readiness**

Approaches to training, briefing and exercising staff and volunteers, ensuring they are confident in their roles and able to respond effectively.

- **Communication and Information**

Templates and guidance for managing information before, during and after an incident, supporting clarity, consistency and public confidence.

- **Physical and Technical Measures**

Scalable options for improving safety and security through site design, equipment, access management and monitoring.

- **Incident Response**

Scenario-based guidance and playbooks to support structured, coordinated responses to a range of potential incidents.

- **Working with Others**

Guidance on multi-agency coordination, Safety Advisory Groups (SAGs), information sharing and the practical realities of operating within a wider system.

- **Governance and Assurance**

Templates and tools to support record-keeping, decision-making and demonstrating a considered, proportionate approach, aligned to risk and context.

What This Toolkit Does Not Assume:

- That risks can be fully predicted
- That complex solutions are always required
- That a single model applies to all environments

Proportionate and Scalable by Design

The Toolkit has been designed to scale.

A small community event may use:

-  a basic risk assessment
-  simple public protection procedures
-  volunteer briefings

A larger or more complex operation may apply:

-  detailed risk modelling
-  structured command arrangements
-  multi-agency coordination and formal planning processes

Both approaches are valid provided they are proportionate to the risk and context.

Alignment with Martyn's Law

The Toolkit intends to align with the expectations of the Terrorism (Protection of Premises) Act 2025 (Martyn's Law), supporting organisations in understanding and applying their responsibilities.

At the time of publication, detailed statutory guidance is still emerging and is expected to evolve as the legislation is implemented in practice.

However, its primary purpose is broader:

To support practical preparedness, informed decision-making and effective coordination — before, during and after an event.

Using the Toolkit in Practice

Organisations may choose to:

-  Use individual sections to address specific needs
-  Integrate templates into existing plans and processes
-  Apply the Toolkit as part of event planning cycles
-  Use it to support internal reviews, exercises or Safety Advisory Group discussions

There is no single “correct” way to use the Toolkit.

Its value comes from how it is adapted, applied and embedded within each organisation's own operational reality.

Application and Benefits

The DSC Toolkit is designed for practical, day-to-day use across the public, private and voluntary sectors.

It supports organisations in translating planning into action helping teams move from understanding risk to making informed decisions in real-world environments.

The Toolkit can be applied at different stages of an event or venue lifecycle, including:

-  **Planning and preparation** - identifying risks, developing proportionate measures and establishing clear procedures
-  **Operational delivery** - supporting briefings, coordination and real-time decision-making
-  **Incident response** - providing structured guidance to help teams act quickly, consistently and with confidence
-  **Review and improvement** - capturing learning and strengthening future readiness

It is equally relevant to:

-  grassroots and community-led events
-  independent venues
-  local authority-led activity
-  large-scale and complex operations

Its value lies not in prescribing a single approach, but in supporting organisations to apply judgement in a structured and defensible way.

Key Benefits

-  **Supports proportionate, risk-based decision-making**
 - Helping organisations focus on what matters most, based on their specific context and capacity
-  **Strengthens preparedness and organisational resilience**
 - Building confidence in how teams plan, respond and recover
-  **Improves coordination across teams and partners**
 - Encouraging shared understanding of roles, responsibilities and communication pathways
-  **Provides practical, usable tools**
 - Templates and guidance designed to be applied in real environments, not just documented
-  **Builds confidence across staff and volunteers**
 - Supporting clear briefings, consistent messaging and effective response

 Reduces reliance on external support

- Enabling organisations to develop and maintain their own internal capability

Wider Integration

The Toolkit forms part of a broader DSC ecosystem, including the Incident Response Playbooks, Event Framing Packs, Responsible Person Training and the National Events Database (NED).

Together, these resources provide additional layers of support, helping organisations to:

- understand their operating environment
- maintain awareness beyond their immediate site
- and strengthen coordination before, during and after events

PART 1: Leadership & The Responsible Person

Leadership and the Responsible Person

Effective preparedness begins with clarity of leadership.

Under the Terrorism (Protection of Premises) Act 2025 (Martyn's Law), certain venues and events are required to designate a Responsible Person. This provides a clear point of accountability for how public protection is considered and applied.

However, in practice, the role extends beyond definition.

The Responsible Person is not simply a title or a point of contact. They are central to how risk is understood, how decisions are made, and how activity is coordinated across teams and partners.

Organisations are not expected to rely on specialist consultants in order to begin preparing. A proportionate, informed approach based on the specific environment is sufficient.

Responsibility in Practice

Responsibility remains constant, but how it is exercised will vary depending on the situation.

In real-world environments, the Responsible Person will:

-  **Understand risk in context** - including factors beyond the immediate site
-  **Maintain oversight** - through information, communication and situational awareness
-  **Coordinate activity** - across internal teams and external partners
-  **Support decision-making** - particularly where information is incomplete or evolving
-  **Account for outcomes** - ensuring decisions are considered, recorded and reviewed

This requires more than knowledge of procedures. It requires the ability to interpret, adapt and respond as conditions change.

Statutory guidance is continuing to develop and may evolve over time. Organisations should ensure their approach is reviewed and adapted as expectations become clearer.

NB: Maintaining a clear decision log supports accountability, continuity and post-incident review, particularly where decisions are made under pressure.

Responsibility, Control and Influence

A useful way to understand the role is through three interacting elements:

-  **Responsibility** - the duty to ensure risks are considered and managed
-  **Control** - the ability to direct actions and resources
-  **Influence** - the ability to shape outcomes through coordination, communication and relationships

These do not always sit in the same place.

At times, the Responsible Person may have direct control. At other times, control may sit with operational teams or external agencies. In these situations, influence - through communication and coordination - becomes critical.

Understanding where control sits, and how to work with it, is central to effective leadership.

The Control Triangle

These three elements **Responsibility, Control and Influence** can be thought of as a simple model - often referred to as the Control Triangle:

-  Responsibility remains constant
-  Control may be held, shared or transferred
-  Influence must be actively used, particularly where control sits elsewhere

Understanding how these interact helps the Responsible Person operate effectively in dynamic environments, where not everything can be directly controlled.

Operating Across Different Levels

The Responsible Person does not move in and out of responsibility but will operate across different levels of decision-making depending on the situation.

This may include:

-  **Strategic involvement** - setting direction, priorities and overall approach
-  **Tactical coordination** - aligning teams, managing developing situations and supporting decision-making
-  **Operational awareness** - maintaining visibility of activity on the ground

Responsibility remains constant, but the way it is exercised adapts to the context.

Leadership in Different Environments

The role will look different depending on scale and complexity.

For a small or community-led event, the Responsible Person may:

-  take a direct role in planning and delivery
-  rely on simple procedures and volunteer briefings
-  coordinate informally with local partners

For larger or more complex operations, the Responsible Person may:

-  operate within structured command arrangements
-  rely on specialist teams and systems
-  engage formally with multiple agencies

Both approaches are valid, provided they are proportionate to the risk and environment.

Key Principle

Effective leadership is not defined by control alone.

It is defined by the ability to:

- understand risk
- recognise where control sits
- coordinate activity
- make informed decisions
- and maintain oversight as situations evolve

PART 2 - People, Training and Readiness

Purpose

Effective preparedness depends on people.

Plans, procedures and tools are only as effective as the individuals applying them. Training and readiness activities help ensure that staff and volunteers:

-  understand their roles
-  recognise risk
-  and are able to respond confidently in practice

This section provides a framework for developing capability in a way that is proportionate, practical and aligned to real-world operations.

A Proportionate Approach to Training

Training should reflect the scale, nature and complexity of the venue or event.

For some organisations, this may involve:

-  basic awareness briefings
-  simple procedures and guidance

For others, it may include:

-  structured training programmes
-  scenario-based exercises
-  multi-agency involvement

There is no single model. The aim is to ensure that:

-  individuals understand what is expected of them
-  training is relevant to the environment
-  and learning can be applied in practice

Core Elements of Training and Readiness

Awareness and Knowledge

Staff and volunteers should have a basic understanding of:

-  the risks relevant to their environment
-  how to recognise suspicious activity or emerging issues
-  how to report concerns

This may include the use of recognised resources such as ProtectUK guidance and ACT Awareness training.

Roles and Responsibilities

Individuals should be clear on:

-  their specific role
-  who they report to
-  how decisions are made and communicated

Clarity reduces hesitation and supports more effective action under pressure.

Procedures and Practical Application

Training should cover key procedures, such as:

-  evacuation, invacuation or lockdown
-  medical emergencies
-  incident reporting and escalation
-  communication protocols

The focus should be on:

-  usability
-  simplicity
-  and consistency

Briefings and Ongoing Readiness

Training is not a one-off activity.

Regular briefings help maintain awareness and ensure that teams remain prepared.

These may include:

-  pre-event briefings
-  shift briefings
-  updates based on changing conditions or risks

Briefings should be:

-  concise
-  relevant
-  and clearly understood

Scenario-Based Learning

Scenario-based learning helps bridge the gap between theory and practice.

This may include:

-  tabletop exercises
-  walkthroughs
-  facilitated discussions
-  workshops

Scenarios do not need to be complex. Even simple exercises can:

-  highlight gaps in understanding
-  test communication and coordination
-  build confidence in decision-making

Scenario-based approaches should complement, not replace, day-to-day operational understanding.

Validation of Process

Training and exercises should be supported by Validation of Process (VoP).

This focuses on how systems operate in practice, particularly under normal conditions, and helps identify:

-  gaps in communication
-  unclear responsibilities
-  assumptions that may not hold in reality

Validation ensures that training is grounded in how the organisation actually operates.

Recording and Demonstrating Readiness

It is important to maintain a proportionate record of training and readiness activity.

This may include:

-  attendance at briefings or training sessions
-  completion of awareness modules
-  participation in exercises or validation activities

Records do not need to be complex, but should be:

-  clear
-  consistent
-  and accessible if required

They support:

-  internal review
-  organisational learning
-  and, where necessary, demonstration of a considered approach

Building Confidence and Capability

The purpose of training is not simply to transfer information, but to build confidence.

Individuals should feel able to:

-  recognise issues
-  take appropriate action
-  communicate clearly
-  and support others

Confidence comes from:

-  clarity of role
-  familiarity with procedures
-  and experience through discussion and practice

Key Principle

Preparedness is strengthened not by the volume of training delivered, but by how well individuals understand their role and apply it in practice.

PART 3 - Working with Others

Working with Others: Coordination and Shared Responsibility

Events and venues do not operate in isolation.

While responsibility may sit with a single individual or organisation, control and influence are often shared across multiple teams, partners and agencies.

Effective preparedness depends on how well these relationships are understood, established and maintained.

These relationships also support shared situational awareness and coordinated communication during both routine operations and incidents.

Why Coordination Matters

In many situations:

-  different organisations hold different pieces of information
-  control may shift depending on the nature of an incident

- decisions need to be made quickly, often across organisational boundaries

Without clear coordination, this can lead to:

- duplication of effort
- gaps in response
- delayed or conflicting decisions

With effective coordination, organisations can:

- share information
- align actions
- and respond more confidently and consistently

Understanding Roles and Responsibilities

Clarity is essential.

Organisations should understand:

- who is responsible for what
- who has decision-making authority
- how escalation works
- where responsibilities overlap

This does not require rigid structures, but it does require shared understanding.

Safety Advisory Groups (SAGs)

Safety Advisory Groups provide a forum for multi-agency discussion and coordination.

They typically include:

- Local Authorities
- Emergency Services
- Regulatory bodies
- Event organisers

SAGs are not decision-making bodies in themselves, but they play an important role in:

-  sharing information
-  identifying risks
-  supporting proportionate planning

Used effectively, they help build alignment before an event takes place.

Please see Appendix G for more information on SAG's.

Working with Emergency Services

Emergency services play a critical role during incidents, and early engagement can significantly improve preparedness.

This may include:

-  sharing plans and layouts
-  agreeing communication methods
-  understanding response expectations

In some situations, control may transfer to emergency services. Understanding how this works in advance helps ensure a smoother and more coordinated response.

Transfer of Control and Primacy

During significant incidents, control may shift between organisations.

For example:

-  from event organisers to emergency services
-  between different responding agencies

This is often referred to as primacy.

The Responsible Person remains accountable for their role, but must be able to:

-  recognise when control has shifted
-  support that transition
-  continue to provide relevant information and coordination

Information Sharing and Communication

Clear, timely communication is essential.

Organisations should consider:

-  how information is shared internally
-  how it is communicated externally
-  how updates are provided during an incident

This includes both:

-  formal communication channels
-  informal, real-time coordination

Coordination in Practice

In practice, effective coordination is built through:

-  early engagement with partners
-  clear and consistent communication
-  shared understanding of roles and expectations
-  regular interaction, not just during incidents

It is not something that can be created in the moment - it must be developed over time.

Key Principle

Responsibility may sit in one place, but effective outcomes depend on how well organisations work together.

PART 4 - Understanding Risk

Effective preparedness begins with understanding risk in context.

Risk is not static and it cannot be reduced to a single document or score. It is shaped by a combination of factors including the nature of the event or venue, the people involved, the surrounding environment and the timing of activity.

For venues and events, this means risk should be considered as part of a wider, evolving picture - not just within the physical boundary of the site.

The aim is not to predict specific threats, but to understand risk in general terms and ensure that proportionate and effective responses can be implemented if required.

In this context, “reasonably practicable” means measures that are appropriate to the size, nature and resources of the organisation, balancing risk reduction with what is realistically achievable.

Looking Beyond the Immediate Site

Many of the factors that influence risk sit outside direct control.

These may include:

-  nearby locations or infrastructure
-  transport routes and public access points
-  concurrent / fringe events or activities
-  wider social or environmental conditions

Understanding this broader context helps organisations anticipate how situations may develop and where additional coordination may be required.

Identifying Threats and Vulnerabilities

Risk assessment involves understanding both:

-  what could happen (threats)
-  where weaknesses exist (vulnerabilities)

Common considerations may include:

-  suspicious items or behaviour
-  unauthorised access
-  crowd density and movement
-  access and egress routes
-  environmental conditions (e.g. weather)
-  reliance on critical infrastructure (power, communications)
-  the presence of vulnerable individuals

The aim is not to predict every possible scenario, but to identify credible risks that could impact safety and operations.

Assessing Risk in Practice

Risk is often considered in terms of:

-  likelihood - how probable an event is
-  impact - the potential consequences if it occurs

However, in practice, these are not always easy to quantify.

A proportionate approach, scaled to the operation, involves:

-  focusing on credible and relevant risks
-  prioritising those with the greatest potential impact
-  recognising uncertainty and avoiding false precision

Judgement plays an important role, supported by experience, local knowledge and available information.

Proportionate Risk Management

Not all risks can be eliminated.

The role of the organisation is to reduce risk to a level that is:

-  reasonable
-  proportionate
-  appropriate to the environment

This may involve:

-  simple procedural measures
-  staff awareness and training
-  physical or technical interventions
-  coordination with external partners

Different environments will require different approaches.

A small community event may rely on:

-  volunteer briefings

-  simple access control
-  clear communication

A larger or more complex operation may require:

-  structured planning
-  layered security measures
-  multi-agency coordination

Both are valid when aligned to risk.

Understanding Risk Appetite

As part of a proportionate approach, aligned to risk and context, organisations should consider their risk appetite - the level of risk they are prepared to accept in order to operate.

This is not about eliminating all risk, which is rarely possible. Instead, it involves making informed decisions about:

-  which risks can be accepted - or not
-  which need to be reduced
-  and which require further action or coordination

Risk appetite will vary depending on:

-  the nature and scale of the event or venue
-  the people attending
-  the environment and context
-  available resources and capabilities

In practice, this may influence decisions such as:

-  whether additional controls or measures are required
-  how access is managed
-  how incidents are escalated
-  when to pause or stop activity

Risk appetite does not need to be formally documented in all cases, but it should be understood and applied consistently when making decisions.

Risk, Control and Decision-Making

Understanding risk is closely linked to understanding control.

In some situations, risks can be directly managed. In others, they depend on factors outside immediate control.

This is where the relationship between:

-  responsibility
-  control
-  and influence

becomes important.

Where control is limited, organisations must rely more heavily on:

-  communication
-  coordination
-  and timely decision-making

Recording and Reviewing Risk

Risk assessment should be documented in a way that is:

-  clear
-  proportionate
-  usable in practice

Documentation should:

-  reflect how decisions have been made
-  support communication with others
-  provide a basis for review and improvement

Risk is not fixed. It should be reviewed:

-  as plans develop
-  during delivery

 after an event or incident

Learning from experience is a key part of strengthening future preparedness.

Key Principle

Risk assessment is not about producing a perfect document.

It is about developing a clear understanding of what matters, and supporting informed, proportionate decisions in real-world environments.

PART 5 - Protective Measures and Public Protection

Once risks are understood, the next step is to determine what can be done to reduce their likelihood or impact.

Protective measures do not need to be complex or resource-intensive to be effective. In many cases, simple, well-understood actions can have a significant impact when applied consistently.

The aim is not to eliminate all risk, but to take proportionate, practical steps that improve safety, support response and build confidence among staff and the public.

A Layered Approach

Effective protection is rarely achieved through a single measure.

Instead, it is built through a combination of:

-  **people** - awareness, behaviour and presence
-  **processes** - procedures, plans and communication
-  **physical and technical measures** - infrastructure, equipment and layout

These layers work together to:

-  deter potential threats
-  detect issues early
-  delay or disrupt harmful actions
-  support an effective response

The balance between these elements will vary depending on the environment and level of risk.

People: Awareness and Engagement

People are often the most effective and adaptable layer of protection.

Staff and volunteers who are:

-  aware of their surroundings
-  confident in their role
-  and clear on what to do

can identify issues early and take appropriate action.

Simple approaches can make a significant difference.

One example is the “Power of Hello” - a straightforward method where staff actively acknowledge visitors through a friendly greeting.

This:

- creates a welcoming environment
- increases natural surveillance
- and can deter or disrupt suspicious behaviour by making individuals aware they have been seen

In many settings, particularly smaller venues or community events, this is one of the most proportionate and effective measures available.

Processes: Clear and Practical Procedures

Procedures provide structure and consistency.

These may include:

-  entry and exit management
-  incident reporting and escalation
-  communication protocols
-  evacuation, invacuation or lockdown arrangements

Procedures should be:

-  simple and clearly understood
-  appropriate to the scale and environment
-  regularly reviewed and practiced

The focus should be on usability, ensuring that procedures can be followed under pressure.

Physical and Technical Measures

Physical and technical measures can support and enhance other layers of protection.

Examples may include:

-  controlled access points
-  barriers or vehicle mitigation measures
-  lighting and visibility improvements
-  CCTV or monitoring systems
-  signage and wayfinding

These do not need to be high-cost or complex. See Part 14 Technical and Physical.

In many cases, small adjustments to layout, visibility or access can significantly improve safety and control.

Proportionate Application

Protective measures should always reflect the level of risk and the nature of the event or venue.

For example:

A small community event may rely on:

-  volunteer awareness
-  simple access management
-  clear communication

A larger or more complex venue may implement:

-  layered physical security
-  structured search procedures
-  dedicated security personnel

Both approaches are valid when they are:

-  proportionate
-  practical
-  and clearly understood

Balancing Safety, Security and Experience

Protective measures should support, not undermine, the overall environment.

Poorly applied measures can:

-  create confusion
-  impact visitor experience
-  or introduce new risks

A balanced approach considers:

-  how measures affect movement and behaviour
-  how they are communicated to the public
-  how they integrate with the overall operation

Effective protection is often visible but not intrusive, reassuring without overwhelming.

Linking Measures to Risk and Decision-Making

Protective measures should not be applied in isolation.

They should be:

-  informed by risk assessment
-  aligned with the organisation's risk appetite
-  supported by clear decision-making

This ensures that measures are:

-  purposeful
-  proportionate
-  and defensible if reviewed

Key Principle

Effective protection is not defined by the number of measures in place, but by how well they work together to support awareness, coordination and response.

PART 6 - Operating Within the Wider Framework

Venues and events operate within a broader landscape of regulation, guidance and oversight.

This may include:

-  licensing requirements
-  local authority processes
-  Safety Advisory Groups (SAGs)
-  health and safety legislation
-  emergency planning arrangements

The Terrorism (Protection of Premises) Act 2025 (Martyn's Law) forms part of this wider picture, but it does not sit in isolation.

A Joined-Up Approach

In practice, organisations are rarely working to a single framework.

Preparedness is most effective when:

-  safety, security and operational planning are aligned
-  information is shared across processes
-  duplication is avoided
-  decisions are consistent and clearly understood

The aim is not to create separate plans for each requirement, but to develop a coherent approach that can be applied across different expectations.

Demonstrating Your Approach

Organisations may be asked to demonstrate how they are managing risk and preparing for incidents.

This may take place through:

-  Safety Advisory Group discussions
-  licensing or planning processes
-  internal reviews
-  engagement with partners or regulators

In these situations, what matters most is not the volume of documentation, but the clarity of your approach.

This includes:

-  understanding of risk
-  proportionate measures
-  clear roles and responsibilities
-  evidence of communication, training and review

Proportionate and Defensible

A proportionate approach should be:

-  **considered** - based on relevant risks and context
-  **practical** - capable of being applied in real environments
-  **consistent** - understood across the organisation
-  **defensible** - supported by clear rationale and decision-making

This does not require perfect information or exhaustive measures, but it does require clear thinking and documented reasoning.

Avoiding Duplication

Many organisations already have:

-  health and safety processes

-  emergency plans
-  operational procedures

Where possible, these should be:

-  aligned
-  updated
-  and integrated

rather than replaced or duplicated.

Key Principle

Preparedness is not about meeting separate requirements in isolation.

It is about developing a clear, proportionate and coordinated approach that can stand up to scrutiny and support effective action when it matters.

PART 7 - Readiness and Assurance Checklist

The following checklist is designed to support organisations in reviewing their preparedness before, during and after an event or period of operation.

It is not intended to be exhaustive, but to provide a practical framework to help ensure that key areas have been considered, applied and, where necessary, can be demonstrated.

This checklist is not exhaustive and should be adapted to reflect the scale, complexity and context of the operation.

This checklist can be used:

-  as part of planning
-  to support briefings
-  during internal reviews
-  or when preparing for external engagement

Before an Event / Operation

Planning and Preparation

- ☐ Risks have been identified and considered in context (including factors beyond the immediate site)
- ☐ Proportionate protective measures have been selected and documented
- ☐ Risk appetite has been considered and applied to decision-making
- ☐ Roles and responsibilities are clearly defined (including the Responsible Person)

Coordination and Engagement

- ☐ Relevant stakeholders and partners have been identified
- ☐ Engagement has taken place where appropriate (e.g. Local Authority, SAG, emergency services)
- ☐ Communication and escalation routes are agreed and understood

People and Readiness

- ☐ Staff and volunteers have been briefed and understand their roles
- ☐ Awareness training has been delivered where appropriate (e.g. ACT Awareness)
- ☐ Key procedures (e.g. evacuation, lockdown, reporting) are understood

Planning and Documentation

- ☐ A proportionate plan is in place (appropriate to scale and risk)
- ☐ Key decisions and rationale have been recorded
- ☐ Templates and tools are prepared and accessible

During an Event / Operation

Situational Awareness

- ☐ Awareness of the operating environment is maintained
- ☐ Changes in risk or conditions are identified and communicated

Coordination and Communication

- ☐ Clear communication is maintained within the team
- ☐ Escalation routes are used where required
- ☐ Information is shared with relevant partners as needed

Decision-Making and Control

- ☐ Decisions are made in a timely and proportionate manner
- ☐ The location of control is understood (internal or external)
- ☐ The Responsible Person maintains oversight, even where control is shared or transferred

Response (if required)

- ☐ Procedures are followed in a way that reflects the situation
- ☐ Actions are coordinated across teams and partners
- ☐ Public safety remains the primary focus

NB: Consideration should also be given to staff and volunteer welfare before, during and after incidents, including fatigue, stress and access to support.

After an Event / Incident

Review and Learning

- ☐ Key actions and decisions are reviewed
- ☐ Feedback is gathered from staff, partners and stakeholders
- ☐ Lessons identified are documented

Recording and Assurance

- ☐ Relevant records are completed and retained
- ☐ Decisions and outcomes can be explained and evidenced if required

Improvement and Adaptation

- ☐ Plans and procedures are updated where necessary
- ☐ Training and briefings are adjusted to reflect learning
- ☐ Improvements are embedded into future planning

Key Principle

Preparedness is demonstrated not only by what is planned in advance, but by how effectively organisations adapt, respond and learn in practice.

PART 8 - Validation of Process

Validation of Process is particularly valuable for organisations with limited resources, as it helps prioritise effort where it will have the greatest impact.

Effective preparedness depends not only on having plans in place, but on understanding whether those plans work in practice.

Validation of Process (VoP) is a structured approach to testing how an organisation operates under normal and disrupted conditions. It focuses on how people, procedures and systems interact in real-world environments.

Rather than testing extreme or unlikely scenarios, Validation of Process examines day-to-day operations (Business as Usual) to identify:

-  gaps in communication
-  unclear roles or responsibilities

-  assumptions that do not hold in practice
-  dependencies that may not be fully understood

Why Validation Matters

Plans that appear clear on paper may not translate effectively into action.

Without validation, organisations may encounter:

-  confusion during incidents
-  delays in decision-making
-  breakdowns in coordination
-  inconsistent application of procedures

Validation helps identify these issues early, when they can be addressed in a controlled environment.

How It Works

Validation of Process is typically delivered through structured workshops or facilitated sessions.

These may involve:

-  walking through key processes step-by-step
-  testing communication and escalation routes
-  exploring how decisions would be made in practice
-  identifying where control, responsibility and influence sit

The focus is not on “passing” or “failing”, but on understanding how the system behaves.

In this context, it is expected - and beneficial - for gaps, friction points or failures to become visible. These provide valuable insight into how processes operate in practice and highlight where clarification, adjustment or additional support may be required.

VoP complements, but does not replace, exercising and readiness activities.

Focus on Business as Usual

A key principle of Validation of Process is that it begins with normal operations.

By understanding how an organisation functions day-to-day, it becomes easier to identify:

-  where disruption is most likely to occur
-  how issues may escalate
-  what additional measures may be required

This provides a more realistic foundation for planning and response.

Link to Planning and Continuity

Validation of Process supports:

-  risk assessment - by identifying real vulnerabilities
-  protective measures - by testing whether they are practical
-  business continuity - by understanding how disruption affects operations
-  incident response - by clarifying roles, decisions and coordination

It ensures that plans are not only documented, but usable and effective.

Embedding Validation

Validation should not be a one-off activity.

It can be incorporated into:

-  planning cycles
-  pre-event preparation
-  internal reviews
-  post-incident learning

Even simple, structured discussions can provide valuable insight.

Key Principle

Preparedness is not proven by what is written in a plan, but by how well it works when applied.

A Validation of Process Workshop Template is included in the appendix - see here.

PART 9 - Readiness, Exercising and Capability

This section builds on training and Validation of Process, focusing on how readiness is developed through structured application.

Preparedness is demonstrated through readiness. While training builds knowledge, readiness is about ensuring that individuals and teams are able to apply that knowledge effectively, particularly in the context of incident response.

This includes:

-  understanding risk
-  recognising developing situations
-  communicating clearly
-  and acting with confidence under pressure

Readiness supports teams by ensuring that plans, procedures and coordination arrangements can be applied in practice, not just understood in theory.

From Training to Readiness

Training provides a foundation, but readiness is developed through application and experience.

This involves moving beyond:

-  awareness
-  procedures
-  and documentation

to ensure that teams can:

-  interpret situations
-  make decisions
-  and coordinate effectively in real time

Readiness should therefore be viewed as an ongoing process, supported by structured activities and regular engagement.

Key Areas of Readiness

1. Risk Awareness

Individuals should understand:

-  the risks relevant to their environment
-  how those risks may present in practice
-  what indicators or triggers may require action

This includes awareness of:

-  suspicious behaviour and hostile reconnaissance
-  environmental factors (e.g: weather, infrastructure failure)
-  operational pressures (e.g: crowds, staffing levels)

2. Role Clarity and Interdependencies

Effective response depends on clarity of roles.

Individuals should understand:

-  their own responsibilities
-  how their role connects to others
-  how decisions are escalated and communicated

This is particularly important where:

-  multiple teams are involved
-  responsibilities overlap
-  or coordination with partners is required

As mentioned in [Part 8 - Validation of Process](#) plays a key role in testing these interdependencies.

3. Procedural Confidence

Teams should be familiar with key procedures, including:

-  incident reporting and escalation
-  evacuation, invacuation and lockdown
-  communication protocols

The focus should be on:

-  usability
-  clarity
-  and confidence in application

4. Readiness Through Exercising

Readiness is best developed through structured activities that simulate real-world conditions. See next section.

Exercising Approaches

A range of exercise formats can be used to support readiness, each offering different levels of complexity, realism and resource requirement.

These approaches should be selected and designed in a way that is:

-  proportionate to the environment
-  aligned to clear objectives
-  and focused on practical learning

Where possible, exercises should:

-  be developed in collaboration with relevant partners
-  focus on specific areas of interest rather than attempting to test everything at once
-  include consideration of the transition from normal operations into response and recovery
-  and incorporate structured learning and follow-up
-  consider returning to normal operations from an incident response and recovery, whether immediate or phased

The value of any exercise lies not in its scale, but in how effectively it improves understanding, coordination and decision-making.

In many cases, a combination of these approaches will provide the most effective route to building and maintaining readiness.

1. Tabletop Exercises

Tabletop exercises are facilitated, discussion-based sessions that explore scenarios step-by-step in a structured environment.

They are particularly useful for:

-  testing decision-making and judgement
-  exploring communication and escalation routes
-  understanding how roles and responsibilities interact

Tabletops can be delivered with minimal resources and are well suited to:

-  smaller teams
-  early-stage planning
-  introducing new concepts or procedures

They also provide a safe environment to:

-  challenge assumptions
-  identify gaps
-  and explore how situations may develop over time
-  introduce injects that change the course of the exercise

Where appropriate, scenarios can include the progression from Business as Usual into an emerging incident, supporting a broader understanding of how response is initiated.

2. Workshops and Walkthroughs

Workshops and walkthroughs provide a more practical, location-based approach to readiness.

They involve:

-  working through processes in the actual environment
-  reviewing physical layouts, access points and movement routes
-  testing how procedures apply in real-world settings

These sessions are particularly valuable for:

- validating roles and responsibilities
- identifying site-specific challenges
- understanding how teams and systems interact in practice

Workshops can also support engagement with partners, helping to:

- align expectations
- clarify communication routes
- and build shared understanding

They are often most effective when focused on specific themes, such as:

- access and egress
- communication
- or incident response procedures
- again injects can be introduced to both layer and test responses

3. Simulations

Simulations introduce a more dynamic and time-sensitive element to exercising.

They typically involve:

- evolving scenarios
- time pressure
- and the introduction of new or changing information (e.g: injects)

This allows teams to:

- test how they respond to developing situations
- practise decision-making under pressure
- and experience the challenges of coordination in real time

Simulations can be scaled depending on need and resource, from:

- simple facilitated scenarios
- through to more structured, multi-team exercises

Where appropriate, simulations should:

-  focus on clear objectives
-  reflect realistic conditions
-  and include the transition from normal operations into incident response

As with all exercise types, the emphasis should remain on:

-  learning
-  adaptability
-  and practical application

4. Live Exercises (Where Practical)

Live exercises provide an opportunity to test procedures and coordination in real-world conditions however they can be both resource and budget hungry.

They can offer valuable insight into how plans operate in practice, particularly in relation to:

-  movement of people
-  use of physical spaces
-  communication under real conditions
-  and interaction between teams and partners

Live exercises should be approached in a way that is proportionate to the scale, complexity and resources of the venue or event.

They are not always necessary, and in many cases, tabletop exercises, workshops or simulations can achieve similar outcomes with less disruption or expense.

Where live exercises are undertaken, the focus should be on:

-  testing key procedures in a controlled and manageable way
-  understanding how people, systems and communication interact
-  identifying practical issues that may not be apparent in planning

Working with Partners

Where opportunities arise to participate in live exercises with emergency services or local partners, these can provide significant value and should be supported where practical.

Early discussion can help ensure that:

-  the objectives of the exercise are clear
-  the level of disruption is understood and managed
-  learning outcomes are shared between participants

Designing for Value

To maximise benefit while avoiding unnecessary burden, organisations should:

-  focus on specific objectives rather than attempting to test all scenarios
-  keep exercises proportionate and relevant
-  use existing staff and resources wherever possible
-  ensure that normal operations are not unduly impacted

The aim is to gain insight, not to create a large-scale simulated incident unless this is appropriate and resourced.

Testing the Full Lifecycle

Where appropriate, organisations should seek to include the period leading up to the simulated incident and then beyond the initial response.

This allows teams to experience the transition from:

-  normal operations (Business as Usual)
-  into incident response (including potential for transfer of control)
-  through recovery
-  and, where appropriate, a return to normality or phased resumption

This end-to-end approach provides a more realistic understanding of how incidents develop and how decisions are made over time.

Learning and Follow-Up

As with all readiness activity, the value of a live exercise is realised through:

-  structured observation
-  capturing lessons identified

 and applying improvements

Even small-scale exercises can provide valuable insight when learning is captured and acted upon.

Different exercise types serve different purposes, but all should be designed to support understanding, improve coordination and build confidence in real-world application.

Communication and Coordination Exercises

Readiness should include testing how teams communicate.

This may involve:

-  use of radios, mobile devices or control systems
-  testing communication chains and escalation routes
-  practising alternative communication methods where systems fail

Clarity, brevity and consistency should be reinforced throughout.

Observation and Awareness Skills

Staff and volunteers should be supported in developing observational awareness.

This includes:

-  recognising unusual or suspicious behaviour
-  identifying unattended items or anomalies
-  understanding when and how to escalate concerns

Resources such as ProtectUK ACT Awareness can support this baseline capability.

Embedding a Culture of Preparedness

Readiness is strengthened by culture.

Organisations should aim to:

-  encourage proactive reporting
-  support open communication
-  reinforce shared responsibility for safety

This includes creating an environment where:

-  individuals feel confident raising concerns
-  learning is encouraged
-  and improvement is continuous

Leadership plays a key role in setting this tone.

Recording and Monitoring Readiness

A proportionate record of readiness activity should be maintained.

This may include:

-  training and briefing records
-  exercise participation
-  validation activities
-  identified gaps and improvements

Records should be:

-  clear
-  consistent
-  and accessible

They support:

-  internal assurance
-  organisational learning
-  and, where required, external engagement

Learning and Continuous Improvement

Readiness activities should be followed by structured review.

This includes:

-  identifying what worked well
-  recognising where gaps or challenges emerged

- 
- capturing lessons and actions

Learning should be:

- 
- documented
-
- 
- shared
-
- 
- and applied to future planning and training

Session Feedback and Evaluation

Feedback is an important part of improving readiness.

After training sessions or exercises, organisations should gather feedback on:

- 
- clarity of content
-
- 
- relevance to the environment
-
- 
- confidence in applying learning
-
- 
- areas for improvement

Feedback mechanisms do not need to be complex, but should:

- 
- encourage honest input
-
- 
- capture practical insights
-
- 
- support ongoing development

Example: Readiness Session Feedback Prompts

Organisations may wish to use simple prompts such as:

- 
- What aspects of the session were most useful?
-
- 
- Do you feel better prepared to respond to an incident?
-
- 
- Were roles and responsibilities clear?
-
- 
- What could be improved or clarified?
-
- 
- What additional support or resources would be helpful?

Key Principle

Readiness is not measured by the amount of training delivered, but by how confidently and effectively individuals and teams can respond when required.

These activities support not only immediate response capability, but also the organisation's ability to sustain operations and recover - explored further in the next section.

PART 10 - Business Continuity Planning

Business Continuity Planning focuses on how an organisation continues to operate when faced with disruption.

For venues and events, disruption can take many forms - from minor operational issues to significant incidents that affect safety, delivery or public confidence.

The aim is not to predict every possible scenario, but to ensure that:

-  critical functions can continue where possible
-  disruption is managed effectively
-  recovery is considered from the outset

Understanding Disruption in Context

Disruption may arise from a wide range of causes, including:

-  loss of power or technical systems
-  staffing shortages or key personnel absence
-  transport or access issues
-  severe weather or environmental conditions
-  safety or security incidents
-  external factors affecting the surrounding area

In many cases, these issues will develop quickly and may affect multiple parts of an operation at the same time.

Identifying Critical Functions

A practical starting point is to identify what is essential to continue operating safely.

This may include:

-  maintaining safe occupancy and crowd management

-  communication with staff, contractors and the public
-  access and egress routes
-  coordination with emergency services or partners
-  critical infrastructure (IT, power, lighting, communications)

Understanding these priorities helps organisations focus their efforts when disruption occurs.

Planning for Continuity

Continuity planning involves identifying how critical functions can be maintained or adapted.

This may include:

-  identifying backup arrangements for key systems or services
-  establishing alternative communication methods
-  planning for reduced staffing levels
-  identifying safe ways to scale down or pause activity if required

Plans do not need to be complex, but they should be:

-  realistic
-  proportionate
-  and clearly understood by those responsible for implementing them

Decision-Making During Disruption

Disruption often requires timely decisions, made with incomplete information.

Organisations should consider:

-  who is responsible for making key decisions
-  how those decisions will be communicated
-  when escalation is required
-  how safety, operations and reputation are balanced

In some situations, this may include decisions to:

- delay or pause activity

- restrict access
- or bring an event or operation to a controlled close

Clarity in advance supports confidence in the moment.

Coordination and Dependencies

Continuity is rarely achieved in isolation.

Many functions depend on:

-  suppliers and contractors
-  utilities and infrastructure
-  transport networks
-  partner organisations

Understanding these dependencies helps organisations:

-  anticipate where disruption may occur
-  coordinate more effectively
-  and respond more quickly when issues arise

Recovery and Return to Normal Operations

Recovery should be considered as part of planning, not just after an incident.

This may include:

-  restoring systems and infrastructure
-  re-establishing normal operations
-  communicating with stakeholders and the public
-  managing reputational impact

Recovery may be phased, depending on the nature and scale of the disruption.

Review and Improvement

After any disruption, there is an opportunity to learn.

Organisations should:

-  review what happened
-  identify what worked well / poorly
-  understand where improvements can be made

These insights should then be used to:

-  update plans
-  improve procedures
-  and strengthen future preparedness

Key Principle

Business continuity is not about maintaining operations at all costs.

It is about maintaining safe, controlled and proportionate operations, and making informed decisions when circumstances change.

PART 11 - Incident Response and Recovery

Even with effective planning and preparation, incidents can still occur.

The purpose of incident response is to ensure that when they do, organisations are able to:

-  act quickly and appropriately
-  coordinate effectively with others
-  protect life and reduce harm
-  and return to safe, stable operations as soon as practicable

Response and recovery should not be viewed as separate activities, but as part of a continuous process that begins the moment an incident is identified.

Recognising and Responding to Incidents

Incidents may vary widely in scale and nature, from minor disruptions to significant emergencies.

Early recognition is critical.

This may involve:

-  identifying unusual behaviour or activity
-  responding to reports from staff or the public
-  recognising changes in the operating environment

Initial actions should focus on:

-  ensuring immediate safety
-  gathering and sharing information
-  activating appropriate procedures

The aim is to stabilise the situation while maintaining clarity and control.

Structured Response

A structured approach supports consistency and coordination.

This may include:

-  following established procedures or playbooks
-  using agreed communication protocols
-  escalating issues in line with defined roles and responsibilities

Where appropriate, organisations may align with recognised frameworks such as the Joint Emergency Services Interoperability Principles (JESIP), including structured information sharing (e.g. M/ETHANE <https://www.jesip.org.uk/joint-doctrine/m-ethane/>).

The level of structure applied should be proportionate to the scale and complexity of the incident.

Decision-Making Under Pressure

Incidents often require rapid decisions, made with incomplete or evolving information.

In these situations, it is important to:

-  prioritise life safety
-  apply proportionate judgement
-  communicate decisions clearly
-  adapt as new information becomes available

Decisions should be:

-  practical
-  defensible
-  and aligned with the organisation's understanding of risk and priorities

Clarity in roles and communication supports confidence in decision-making.

Responsibility, Control and Coordination

During an incident, the relationship between responsibility, control and influence becomes more visible.

-  Responsibility remains with the organisation and the Responsible Person
-  Control may sit with operational teams or transfer to external agencies
-  Influence is exercised through coordination, communication and information sharing

Understanding how these interact helps ensure a more effective and coordinated response.

Working with Emergency Services

In more serious incidents, emergency services may take a leading role.

This may involve:

-  transfer of operational control
-  coordinated multi-agency response
-  structured communication and decision-making

The organisation should be prepared to:

-  recognise when this transition occurs
-  support it effectively
-  continue to provide relevant information and assistance

Early and clear communication supports a smoother transition.

Communication During an Incident

Clear communication is essential.

This includes:

-  internal communication with staff and volunteers
-  coordination with partners and agencies
-  communication with the public where appropriate

Information should be:

-  accurate
-  timely
-  consistent
-  clear and concise

Even simple, clear messages can significantly improve response effectiveness.

Recovery and Return to Operations

Recovery begins during the response phase.

It involves:

-  restoring safe operating conditions
-  supporting affected individuals
-  re-establishing normal activity where appropriate

Recovery may be gradual and should take account of:

-  safety considerations
-  operational capability
-  stakeholder confidence

In some cases, recovery may include a phased return or changes to how operations are delivered.

Learning from Incidents

Every incident provides an opportunity to learn.

Organisations should:

-  review actions taken
-  identify what worked well
-  understand where improvements are needed

This learning should be used to:

-  update plans and procedures
-  inform training and briefings
-  strengthen future preparedness

Key Principle

An effective response is not defined by the absence of disruption, but by how well an organisation adapts, coordinates and acts under pressure.

PART 12 - Collaboration and Coordination Tools

Effective response depends not only on planning and leadership, but on how well individuals and organisations are able to work together in real time.

Coordination is supported by a range of practical tools and approaches that help teams:

-  share information
-  align actions
-  and maintain a common understanding of the situation

These tools do not need to be complex, but they do need to be:

-  understood
-  used consistently
-  and applied in a way that reflects the scale and nature of the event or incident

Shared Situational Awareness

A common understanding of what is happening is essential.

This is often referred to as ‘situational awareness’.

It involves:

-  understanding the current situation
-  recognising how it may develop
-  and sharing that understanding with others

This may be achieved through:

-  regular updates or briefings
-  use of control points or coordination hubs
-  clear reporting structures
-  a daily rhythm (see note below)

Maintaining a shared picture helps ensure that decisions are:

-  aligned
-  timely
-  and based on the best available information

Maintaining Awareness: Rhythm and Routine

Situational awareness is most effective when it is actively maintained, rather than assumed.

This can be supported through a simple operational rhythm, including:

- regular check-ins or briefings
- short “huddles” or “scrums” at key points during the day or event
- defined update intervals for teams and supervisors

These touchpoints provide an opportunity to:

- share updates on current conditions
- identify emerging risks or issues
- confirm priorities and actions
- reinforce communication across teams

Huddles do not need to be formal or time-consuming. In many cases, short, focused updates can significantly improve shared understanding and coordination.

Establishing a simple operational rhythm - including regular briefings, huddles or scrums - helps ensure that situational awareness is maintained and shared across teams. These should be short, focused and aligned to key decision points or changes in activity.

Structured Communication

During incidents, structured communication helps reduce confusion and improve clarity.

Where appropriate, organisations may adopt recognised approaches such as:

-  Joint Emergency Services Interoperability Principles (JESIP)
-  Structured reporting formats such as M/ETHANE

These provide a consistent way of sharing critical information, including:

-  what has happened
-  where it has happened
-  the scale and nature of the incident
-  what actions are being taken
-  what support is required
-  decision logs that include contemporaneous and or retrospective records

Even where formal structures are not used, applying the same principles - clarity, brevity and consistency - can significantly improve communication.

Roles and Coordination Structures

Clear roles support effective coordination.

Depending on the scale of the event or incident, this may include:

-  a single point of coordination (e.g: event control or duty manager)
-  defined roles for communication, operations and safety structured approaches such as Gold / Silver / Bronze or Strategic / Tactical / Operational - (see note on Naming Conventions and Terminology below)

Not all events require formal structures, but all benefit from:

-  clarity of responsibility
-  understanding of decision-making authority
-  defined escalation routes

Naming Conventions and Terminology

In practice, different organisations and sectors may use different terminology to describe similar roles and levels of responsibility.

For example:

-  Emergency services and some public sector organisations commonly use Gold / Silver / Bronze to describe Strategic, Tactical and Operational levels of command
-  Event and venue teams may use terms such as Event Control, Operations, Duty Manager, or Supervisor
-  Contractors and suppliers may have their own internal role titles and structures

While the terminology may vary, the underlying functions are often similar:

-  Strategic - setting overall direction and priorities
-  Tactical - coordinating activity and managing resources
-  Operational - delivering actions on the ground

It is not essential for all organisations to adopt the same naming conventions. However, it is important that:

-  roles and responsibilities are clearly defined
-  decision-making authority is understood
-  communication routes are agreed
-  and terminology is clarified where multiple organisations are working together

Where possible, aligning or mapping roles across organisations can help reduce confusion, particularly during incidents involving multiple agencies.

Variation in Terminology: Tactical and Operational

In some sectors, particularly within events and venues, the terms “Tactical” and “Operational” are sometimes used interchangeably, or in a different order to that used by emergency services.

In some event environments, “Operational” may be used to describe what would traditionally be considered a tactical or coordination role, while “Tactical” may be used less consistently or not at all.

This variation can lead to confusion, particularly when multiple organisations are working together.

To reduce this risk, it is helpful to focus on function rather than terminology:

-  Strategic - setting overall direction and priorities
-  Tactical - coordinating activity and managing resources
-  Operational - delivering actions on the ground

Where different naming conventions are in use, organisations should:

-  clarify roles at the outset
-  confirm who is making decisions at each level
-  ensure communication routes are clearly understood

Information Flow

Effective coordination depends on how information moves between people and organisations.

This includes:

-  upward reporting (from operational teams to decision-makers)
-  downward communication (from leadership to teams)
-  lateral sharing (between teams and partners)

Information should be:

-  relevant
-  timely
-  and actionable
-  recorded

Too much information can be as challenging as too little. The focus should be on what is needed to support decisions and action.

Communication Planning and Messaging

Effective communication underpins all aspects of preparedness, response and recovery.

A structured communication approach helps ensure that information is:

-  clear
-  timely
-  and understood by those who need to act on it
-  accurately included in decision logs

This applies across:

-  normal operations (Business as Usual)
-  developing situations
-  incidents and emergencies
-  and post-incident recovery

A proportionate communication plan supports the whole team in coordinating activity, maintaining situational awareness and engaging with internal and external stakeholders.

Purpose of a Communication Plan

A communication plan provides a clear framework for how information will be:

-  shared internally
-  communicated externally
-  and managed throughout the lifecycle of an event or incident

The aim is not to create a complex document, but to ensure that:

-  key messages are consistent
-  roles are understood
-  and communication supports effective decision-making

Core Elements

Objectives

Communication should support:

-  safety of staff and the public
-  accurate and timely information sharing
-  coordination with partners
-  maintenance of public confidence

Audiences

Organisations should identify key audiences, including:

-  Internal: staff, volunteers, contractors, security teams
-  External: attendees, emergency services, local authorities, media and the public

Understanding who needs information - and when - supports more effective communication.

Roles and Responsibilities

Clear roles help ensure communication is coordinated and consistent.

These may include:

-  **Responsible Person**
 - Maintains oversight and supports key decision-making
-  **Spokesperson**
 - Leads external communication, particularly with media and public audiences
-  **Communication Coordinator**
 - Manages the dissemination of messages across channels
-  **Team Leads / Supervisors**
 - Relay information to operational staff and volunteers
-  **Loggist / Scribe**
 - Records decisions, actions and key communications

In smaller organisations, these roles may be combined, provided responsibilities remain clear.

Communication Tools and Channels

Organisations may use a range of communication methods, including:

-  radios or on-site communication systems
-  mobile phones and messaging platforms
-  control rooms or coordination centres
-  public address systems

It is important to:

-  understand the strengths and limitations of each
-  have contingency options where possible
-  ensure that key individuals know how to use them

Consistency in how tools are used is often more important than the technology itself.

Organisations should identify and plan for how communication will take place.

Internal Channels

-  radios or communication systems
-  mobile messaging platforms (e.g. SMS or group messaging tools)
-  public address systems or loud hailers
-  Back-up channels in case primary channels fail (see Resilience and Redundancy below)

External Channels

-  direct contact with emergency services and partners
-  social media platforms
-  SMS alerts or attendee communications
-  media statements

Resilience and Redundancy

Communication systems may fail or become overloaded.

Organisations should consider:

-  backup communication methods (including analogue systems)

-  alternative channels
-  limitations of mobile networks during peak demand

The aim is to ensure continuity of communication, even in degraded conditions.

Messaging and Communication Tools

1. Pre-Event Communication

Clear communication before an event helps establish expectations and readiness.

This may include:

- establishing relationships with partners
- agreeing communication methods
- understanding roles and expectations
- testing arrangements through briefings or validation activities
- staff and volunteer briefings
- attendee information (e.g: access, safety information, site rules including prohibited items)
- use of social media and event communications

2. Incident Messaging

During an incident, communication should be:

- clear
- concise
- and focused on action

Pre-prepared messages can support consistency.

Examples may include:

- evacuation instructions
- lockdown or shelter guidance
- reassurance and updates

Messages should avoid speculation and be aligned with partners where appropriate.

3. External Communication and Media

Communication with external audiences should be:

- accurate
- timely

- coordinated

This includes:

- preparing holding statements
- aligning messaging with emergency services and authorities
- avoiding attribution of blame or unverified information

The DSC Incident Response Playbook provides further guidance on managing media and press engagement.

4. Contacts and Information Management

Maintaining up-to-date contact information is essential.

This may include:

- internal team contacts
- emergency services
- local authorities and partners
- key suppliers and resources

Information should be:

- accessible when needed
- securely stored
- managed in line with data protection requirements

5. Communication During an Incident

During an incident, coordination relies on:

-  clear leadership
-  shared understanding
-  structured communication
-  and adaptability as the situation evolves

A structured approach supports clarity and coordination. This may include:

- **Identification and escalation**
 - Recognising issues and ensuring they are reported appropriately
- **Information verification**
 - Confirming accuracy before wider dissemination
- **Message dissemination**

- Selecting appropriate channels and formats
- **Structured reporting**
 - Using recognised formats such as M/ETHANE (see note below) where appropriate
- **Feedback and confirmation**
 - Ensuring messages are received and understood
- **Recording and logging**
 - Capturing key decisions and actions
- **Horizon scanning**
 - Monitoring internal and external impacts
- **Understanding primacy**
 - Recognising when control transfers to emergency services and how to support this
- **Standing down**
 - Determining when it is appropriate to return to normal operations

M/ETHANE:

NB: The declaration of a MAJOR incident is likely to be made by the emergency services; event organisers should only refer to a 'possible' MAJOR incident.

- **M – Major incident** declared (Yes / No)
- **E – Exact location** of the incident
- **T – Type of incident** (e.g: fire, explosion, structural collapse)
- **H – Hazards** present or suspected (e.g: fire, chemicals, risk of collapse)
- **A – Access** routes to the scene (e.g: safest entry / exit points)
- **N – Number** of casualties or potential casualties
- **E – Emergency services** required (e.g: police, fire, ambulance, specialist units)

6. Post-Incident Communication

This may include:

- internal debriefs and structured review
- updates to stakeholders and attendees
- media engagement where appropriate
- follow-up communication with partners and authorities

7. Review and Continuous Improvement

Communication arrangements should be:

- reviewed regularly
- tested through exercises

- updated following incidents or learning

This helps ensure they remain relevant and effective.

Radio Communication

Where radio systems are used, clear and consistent voice procedures support effective communication.

Key principles include:

- keep messages brief and operationally focused
- speak clearly and avoid unnecessary language
- confirm receipt and understanding
- avoid sharing sensitive or confidential information

Simple, consistent protocols help reduce confusion and improve coordination.

Effective communication is not defined by the volume of information shared, but by how clearly and consistently it supports understanding, decision-making and action.

Voice Procedures

Basic radio discipline helps ensure messages are understood first time and reduces unnecessary traffic.

Key principles include:

- press – pause – speak
- keep messages brief and operationally focused
- speak clearly and at a steady pace
- wait for others to finish before transmitting
- avoid slang, jargon or unnecessary language
- do not share sensitive or confidential information over open channels

Where messages are longer or more complex, consider moving to an alternative channel or communication method (e.g: mobile phone).

Use of Radio Terminology

Traditional radio terminology such as:

- “over” (I expect a response)

- “out” (no response required)
- “say again” (repeat message)
- “standby” (wait)
- “priority message” (other users should respect this call could take priority)

These can help structure communications and are still widely recognised, particularly in multi-agency environments.

NB: In multi-agency environments, more formal terminology may be adopted to align with partner organisations.

However, many modern radio systems - and event environments - operate effectively without strict use of this terminology.

In these cases, clarity and brevity are more important than formal phrasing.

Simple, plain language communication is often sufficient, provided that:

- messages are clear
- responsibility for responding is understood
- and confirmation is given where required

Consistency of Approach

Whichever approach is adopted, it should be:

- consistent across the team
- understood by all users
- and appropriate to the scale and complexity of the operation

Where multiple organisations are working together, it may be helpful to:

- agree a common approach in advance
- or adopt more structured terminology where appropriate

Example Call Structure

A simple, effective call structure may include:

- identifying who you are calling
- identifying yourself
- delivering a clear, concise message
- confirming receipt where needed

For example:

“Control, this is Gate 2”

“Gate 2, Control - pass your message”

“Gate 2, access queue building, request additional support from the stewarding team.”

PART 13 - Technical and Physical Security

Below are measures highlighted by ProtectUK <https://www.protectuk.police.uk/> and the Home Office, Plus, practical, affordable options for grassroots organisations:

Key Benefits:

- By implementing these measures, organisations can improve safety and reduce risks effectively, regardless of their size or resources
- This approach aligns with Martyn’s Law’s aim of promoting proportionate, reasonable and practical actions (subject to further guidance from the Home Office)

1. Security Equipment and Maintenance

Lighting:

- Ensure good lighting, especially around entrances, exits and public areas, to deter suspicious activity and aid CCTV coverage
- Use motion-detecting or dusk-to-dawn lights to enhance security and save energy

Alarms:

- Install a working alarm system that can alert on-site staff and emergency services to potential threats
- Ensure alarms are installed by certified contractors

CCTV:

- Position cameras to minimise blind spots and ensure sufficient lighting for effective night-time recording
- Display clear signage to act as a deterrent and comply with GDPR

2. Technology Integration Resources

Larger venues and events may be able to leverage modern security technologies:

- Surveillance systems, including face recognition CCTV camera placement and monitoring best practices & regulations
- Use and control of drones

- Information on integrating real-time threat monitoring apps or software or subscription to the Decision Support Centre (DSC)
<https://www.decisionsupportcentre.com>
- Guidance on data privacy and GDPR compliance when using technology

3. Physical Security Measures



Perimeter Security:

- Use PAS rated barriers or bollards to prevent unauthorised vehicle access at key entry points (PAS stands for Publicly Available Specification such as ISO PAS 68, or international standard ISO IWA 14-1:2013, CEN CWA 16221:2010, BSI PAS 170-1:2017) See link to [NPSA](#) leaflet.
- Regularly inspect fencing, gates and locks for vulnerabilities and possible interference



Doors and Locks:

- Secure external doors with robust locks and consider door reinforcement options, such as film for glass panels or door bolts
- For venues with older doors, custom fittings, furniture or barricades can serve as temporary reinforcement during emergencies

4. Crowd Management Tools



Organisers should ensure safe movement and gathering of large crowds:

- Use guidance and tools for calculating crowd density and flow rates (see the Purple Guide and Green Guide for more information)
- Refer to guidance on positioning staff and barriers to manage queues and bottlenecks
- Use incident response protocols for crowd surges or panic scenarios
- Maintain contact with neighbours and stakeholders in case of incident

5. Access Control



Event Access Management:

- Consider the use of wristbands, tickets, or passes to control who enters your event
- Maintain a visitor log for closed events to track attendance
- Conduct inductions for visitors and staff



Staff and Volunteer Identification:

- Equip staff and volunteers with suitable accreditation to prevent unauthorised access to restricted areas

6. Communication Tools (see also [PART 12](#))



Public Address Systems:

- Use PA systems for timely announcements in emergencies (consider loud hailers as a back-up)

 Two-Way Radios:

- Provide staff with radios to maintain effective communication

7. Cost-Effective Measures for Grassroots Organisations

 Good Housekeeping:

- Keep public areas clean and clutter-free to reduce hiding places for suspicious items
- Inspect bins and other external areas regularly for signs of tampering or reconnaissance

 Visible Deterrents:

- Simple measures like clear signage (“CCTV in use” or “Security patrolled”) can deter potential threats

 Temporary Barriers:

- Use cones, temporary fencing, or volunteer marshals to manage crowds and access points

8. Additional Resources

- 
- Refer to the
- ProtectUK**
- <https://www.protectuk.police.uk/>
- platform for more detailed advice on physical security measures tailored to both standard and enhanced duty premises



Look up case studies from similar venues for practical examples of implementing these measures

PART 14 - Hostile Vehicle Mitigation (HVM) and Traffic Management

This section outlines the measures that can be implemented to protect attendees, staff, and the public, in accordance with guidance from the National Protective Security Authority (NPSA), the National Counter Terrorism Security Office (NaCTSO) and the protective principles underpinning Martyn’s Law (subject to further guidance from the Home Office).

It also provides awareness of and readiness for Temporary Traffic Regulation Orders (TTROs) and Anti-Terrorism Traffic Regulation Orders (ATTROs), which may be issued by law enforcement to support public protection.

Temporary Traffic Regulation Orders (TTROs)

Purpose:

Used to temporarily prohibit or restrict traffic (including vehicles or pedestrians) for planned works or events. Often the foundation for your event's road or traffic plan. May be used in conjunction with HVM plans (e.g: barriers across closed roads). TTROs are pre-planned and public-facing. TTROs are applied for by event organisers via the local highway authority.

Used For:

- Road closures for festivals, parades, sporting events
- Creating pedestrian-only zones
- Temporary speed restrictions

Legal Basis: Road Traffic Regulation Act 1984 (Sections 14 and 16A)

Hostile Vehicle Mitigation (HVM) refers to strategies and physical measures designed to deter, delay, or prevent the use of vehicles as weapons in attacks on crowded public spaces or events. Such attacks involve vehicles being driven into pedestrians or used to breach barriers and gain access to restricted areas. Often, these sorts of attacks are the first phase of a multi-tiered attack.

Key Benefits of HVM

- 🌀 Creates a physical and psychological deterrent for potential attackers
- 🌀 Ensures safer public spaces by minimising the risk of vehicle-based incidents
- 🌀 Aligns with Martyn's Law recommendations for reasonable and practical safety measures (subject to further guidance from the Home Office)

The following measures should be considered as part of a site-specific risk assessment:

- 🌀 Physical vehicle barriers (temporary or permanent)
- 🌀 Controlled vehicle entry points with staff presence
- 🌀 Security stewarding and vehicle marshals
- 🌀 Timed vehicle movement zones (e.g: for build, re-supply or breakdown)
- 🌀 External signage and route demarcation
- 🌀 Pedestrian-only zones near key crowd density areas
- 🌀 Supplier and contractor briefings on vehicle safety protocols

Why HVM Matters

HVM is crucial for safeguarding venues, events and public spaces from vehicle-borne threats, including:

 **Intentional Acts:** Deliberate use of vehicles in attacks.

 **Accidental Incidents:** Unintended breaches that could still result in harm.

Effective HVM measures can reduce risks and enhance the safety of attendees, staff and infrastructure.

Important considerations:

-  HVM may require planning consent from local authority due to its location, size or weight and period of deployment
-  Impact on underground services – also due to access, size and weight
-  Services access (manholes, street cabinets, as well as access for services vehicles inside any cordon)
-  In support of HVM, a key legal instrument available to police and local authorities is the Anti-Terrorism Traffic Regulation Order (ATTRO), a power introduced under the Counter-Terrorism and Border Security Act 2019. (See section [below](#)).

Simple Measures to Deter and Defend Against Vehicle Attacks:

1. Physical Barriers:

-  **PAS / ISO rated Bollards and Barriers:** Install fixed or temporary bollards to restrict vehicle access. Bollards should be spaced closely enough to prevent vehicle entry while allowing pedestrian flow.
-  **Concrete Blocks or Planters:** Use heavy, immovable objects like reinforced planters or water-filled barriers as temporary protective measures.

2. Perimeter Security:

-  Create vehicle-free zones by limiting access to authorised vehicles only.
-  Use gates, fences, or temporary cordons to clearly define pedestrian-only areas.

3. Access Control:

-  Deploy security personnel to check vehicles entering restricted zones.
-  Use chicanes, retractable barriers or spikes to control entry points.

4. Traffic Management:

-  Redirect traffic away from high-risk areas during events.
-  Use road closures or one-way systems to limit vehicular movement near crowded spaces.
-  Segregate vehicles and pedestrians.

5. Signage and Deterrence:

-  Install visible signage indicating restricted vehicle zones.

-  Highlight the presence of security measures, such as barriers and surveillance systems.

6. **Surveillance:**

-  Monitor access points with CCTV to detect unauthorised vehicle activity.
-  Position security teams strategically to respond quickly to threats.

7. **Vehicle Screening:**

-  For events requiring vehicle access (e.g: porterage, shuttle buses, re-supply vehicles), conduct stops and / or inspections to verify authorisation and check for potential threats.

Considerations for Grassroots and Smaller Organisations

-  **Affordable Options:** Use water-filled barriers, large planters, 1-ton bags filled with soil or parked vehicles as temporary barriers for events on limited budgets.
-  **Community Support:** Coordinate with local authorities for temporary road closures or barrier installation.
-  **Training:** Educate staff and volunteers on recognising suspicious vehicle behaviour and responding to incidents.
-  **Refer to:** The National Barrier Asset team for further advice.

Hostile Vehicle Mitigation and Anti-Terrorism Traffic Regulation Order (ATTROs) – Understanding the Legal and Operational Context

Background

Hostile Vehicle Mitigation (HVM) is a critical strand of protective security planning, particularly for events or venues that involve pedestrianised public areas or crowded spaces. It refers to the range of physical and procedural measures designed to deter or prevent the use of a vehicle as a weapon; a tactic increasingly used in acts of terrorism and criminal disruption.

In support of HVM, a key legal instrument available to police and local authorities is the Anti-Terrorism Traffic Regulation Order (ATTRO), a power introduced under the Counter-Terrorism and Border Security Act 2019. This Act amends the Road Traffic Regulation Act 1984.

What is an ATTRO?

An ATTRO is a legal order made by a Chief Officer of Police, which allows for traffic regulation measures to be imposed (or held in reserve) for the purpose of avoiding or reducing danger connected with terrorism and implemented by a traffic authority (for

example Local Authorities or Highways England). Approximately 40 ATTROs are made annually.

This may include:

-  Road closures or diversions
-  Parking suspensions or restrictions
-  Vehicle access restrictions at certain times or in specific zones
-  Holding powers for “on-demand” closures during an unfolding threat

Unlike conventional Temporary Traffic Regulation Orders (TTROs), ATTROs can be activated with very short notice or held as a precautionary measure, often without disclosing full operational reasoning (to avoid compromising sensitive intelligence or counter-terrorism operations).

When Are ATTROs Relevant to Organisers?

Event organisers and venue operators may need to engage with the concept of ATTROs in any of the following scenarios:

-  Large public gatherings in open public areas or city centres
-  Events located near high-profile or high-risk premises
-  Events where crowd movement crosses vehicular roads
-  Sites with significant VIP attendance or high media visibility
-  Events designated as part of a pre-planned policing operation

In such cases, the police may request an ATTRO to support protective security, particularly where vehicle exclusion zones or flexible “stop and hold” powers are deemed necessary.

Organisers may need to meet the cost of the ATTRO – the cost can range from a few hundred pounds to thousands depending on the complexity of the order.

Organisers do not request an ATTRO directly, the power rests with the police, but they may be asked to support its implementation or communicate its impact to contractors, residents, and attendees.

Operational Implications for Organisers

If an ATTRO is likely to apply to your event:

-  Liaise early with your Safety Advisory Group (SAG), police and local authority traffic management teams.

-  Factor in traffic disruptions, vehicle exclusion and alternative access routes into your site and crowd planning.
-  Prepare contractor and supplier access protocols (e.g: timed entry, security vetting).
-  Plan for clear steward and signage communication to prevent confusion during activation or adjustment.
-  Consider the impact on disabled access, local businesses and emergency vehicle entry.
-  Include ATTRO related information in your risk assessment and security plan documentation.

ATTROs and Martyn's Law

While ATTROs are not a requirement under Martyn's Law, their use supports the reasonable and practical security measures expected of venues and events under the law and very likely within the Enhanced Tier.

Their existence underscores the need for close collaboration with local policing units and for dynamic, joined-up traffic and crowd risk planning.

If your event qualifies for Martyn's Law, particularly in the Enhanced Tier, you should demonstrate:

-  Awareness of ATTROs as a security tool
-  An ability to coordinate with law enforcement and adapt plans accordingly
-  A willingness to incorporate ATTROs and other police-led mitigation into your risk framework

DSC Recommendations

-  Include an HVM section in your Security Plan referencing potential ATTRO requirements.
-  Brief your team on the meaning and use of ATTROs, especially if operating in urban or vehicle-accessible environments.
-  Maintain open communication with your local counter-terrorism security advisor (CTSA) or designated police contact to understand the local threat context.

PART 15 - Other important considerations

Emergency Traffic Regulation Notices

Purpose: Immediate short-term restrictions (e.g: emergency road closures).

Legal Basis: Also under the Road Traffic Regulation Act 1984.

Used For: Sudden infrastructure failure (bridge collapse, flooding), Policing incidents

Duration: Up to 21 days without formal consultation.

Why it matters: May disrupt your event unexpectedly or be initiated by authorities in reaction to unfolding incidents.

Section 14 Public Order Act 1986

Purpose: Allows police to place conditions on public assemblies or marches that may cause serious disruption or disorder.

Authority: Chief constable (or above) can impose conditions relating to location, timing, or numbers.

Used For: Protest marches near venues, high-profile gatherings deemed at risk of disorder.

Why it matters: If your event is high-profile or adjacent to a protest, this legislation may be used to adjust crowd flow, restrict public access or initiate contingency plans.

Civil Contingencies Act 2004 – Emergency Powers

Purpose: Framework for major incident planning and inter-agency cooperation.

Used For:

-  Multi-agency response to large-scale disruption (terrorism, natural disasters)
-  Relevance: While not directly invoked by event organisers, understanding this framework supports Martyn's Law readiness and aligns with the JESIP (Joint Emergency Services Interoperability Principles).

Why it matters: Your emergency planning and control room coordination may plug into this framework in a serious incident.

Planning Conditions and Licensing Restrictions

Scope: While not specific traffic powers, your premises licence, event licence or planning consent may contain:

-  Mandated access controls
-  Restricted delivery times

-  Steward-to-attendee ratios
-  Requirement for police sign-off

Why it matters: Overlapping with TTROs and ATTROs, these may inform or limit your options around HVM and vehicle control.

Designated Protection Zones (DPZ) (upcoming and subject to further guidance)

-  While not yet legislated as separate zones, Martyn's Law (2025) empowers regulators and police to expect protective security zones, especially in Enhanced Tier locations.
-  Future ATTRO-like mechanisms may emerge to support compliance or inspection regimes for known high-footfall venues.

Why it matters: Stay alert to further Home Office or policing guidance on designated 'vulnerability' zones where fast vehicle intervention may be required.

PART 16 - Policies and Documents

Aim:

This focuses on the essential documents and templates that venues and event organisers need to consider.

Key Benefits of Policies and Documents Section

-  **Streamlined Compliance:** Provides venues with ready-to-use tools for meeting legal requirements
-  **Risk Mitigation:** Encourages proactive planning and documentation to prevent and respond to incidents
-  **Regulatory Confidence:** Amongst other measures ensures venues can show they are prepared for inspections

1. Readiness Review

See Appendix E

Checklist Items:

- Risk assessment completed and documented
- Public Protection / Security plans and emergency procedures in place
- **Responsible Person** nominated

- Staff and volunteer training conducted
- Communication protocols tested
- Insurance cover in place and event within insured period
- All documents reviewed and updated within the past year
- Event or Venue listed on the National Events database ([see link](#))
- See also [PART 1](#)

2. Public Protection Procedures

See DSC Security Plan Templates

Purpose: A foundational document outlining the organisation's commitment to safety and security

Key Components:

- **Policy Statement:** A declaration of the organisation's intent to prioritise safety and security
- **Scope:** Define the venue(s), events, audience and staff covered by the policy
- **Roles and Responsibilities:** Detail the duties of the **Responsible Person**, staff and volunteers
- **Review:** Specify how often the policy will be reviewed and updated (eg: annually)
- **Emergency Procedures Plan**
 - **Evacuation Plan:** Maps of exits, assembly points and routes
 - **Lockdown Procedures:** Steps to secure the venue during a threat
 - **Communication Plan:** Scripts and contact protocols for notifying staff and attendees. (see also [Chapter 4](#) Communication Template)
- **First-Aid Response:** Locations of medical kits and roles of designated responders
- Location of nearest medical facilities (eg: hospitals)

Tip – Use: DSC Basic Security Plan Template, Enhanced Tier Security Plan Template. Refer to the NPSA guidance:

<https://www.npsa.gov.uk/resources/npsa-evacuation-lockdown-and-invacuation-guidance>

3. Risk Assessment Record

 **Purpose:** Document the process of identifying, evaluating and mitigating risks.

To include:

- **Event Details:** Name, date, location and organiser
- **Threat Analysis:** List potential risks (e.g: terrorism, crowd surges) with likelihood and impact ratings

- **Mitigation Measures:** Actions taken to reduce risks, such as training, bag searches, additional barriers, evacuation & lockdown plans
- **Reviewer Details:** Full name and signature of the person conducting the assessment

Tip - Use: the DSC Risk Assessment Template

4. Training and Competency Records

 **Purpose:** Track staff and volunteer participation in required training programs

 **Components:**

- Names and roles of attendees
- Date, type and duration of training (e.g: ACT Awareness <https://www.protectuk.police.uk/learning> & first aid)
- Certificates or proof of completion
- Schedule for refresher training

5. Generic Checklists for each phase of the event

Planning Phase

Remote / Hybrid or Office based / meetings / site visits:

- Decide what the event will be
- Set the budget
- Book suppliers
- Get permissions
- Sort logistics

Local Authority & likely compliance checks

- Martyn's Law Tier identified and notified
- Where applicable notify the Local Authority (LA) and / or Safety Advisory Group (SAG) with required documentation.
- All planning or land use permissions granted (temporary structures, signage, land use)
- Road closures, diversions and traffic management plans approved and signage in place
- Noise management plan in place and monitoring equipment set up
- CT Risk Assessment
- Responsible Person identified
- Event listed on the National Events Database

Utilities

- Power, Water, Waste management arrangements confirmed:

- Power – Metering & readings, Electrical Installation Condition Report (EICR) or Temporary Electrical Installation Certificate obtained and filed
- Water - Water quality testing, food grade storage tanks
- Waste - Bins and recycling points deployed

Licensing & Permits

- Premises Licence / Temporary Event Notices (TENs) granted and displayed – see note on Alcohol Licensing below.
- Alcohol licence conditions met, Designated Premises Supervisor (DPS) in post; staff trained.
- Public entertainment licence in place (music, performance, film screenings).
- Street trading licences issued for all vendors or concessions.
- Food safety compliance confirmed, vendor hygiene certificates, allergen labelling, EHO sign-off.
- Pyrotechnics / special effects licences granted; suppliers vetted, insured and briefed.

Alcohol Licensing

1. Know Your Licence

- If you're selling alcohol, you must have either a:
 - Premises Licence. See: <https://www.gov.uk/find-licences/premises-licence>
 - or a Temporary Event Notice (TEN). See: <https://www.gov.uk/find-licences/temporary-events-notice>
- One person must be the Designated Premises Supervisor (DPS) if under a Premises Licence, they will hold a Personal Licence.
- Check and follow all licence conditions, these might limit hours, types of drinks, or require extra security.

2. Age Verification – Challenge 18 / Challenge 25

- Challenge 18 = anyone who looks under 18 is asked for ID.
- Challenge 25 = anyone who looks under 25 is asked for ID. (This is now the more common approach and strongly recommended by the police and trading standards.)
- Acceptable ID:
 - Passport
 - UK / EU photo driving licence
 - PASS-accredited proof-of-age card
(Always check photo, date of birth, and hologram security mark)

3. Serving Alcohol – Do's & Don'ts

DO

- Display Challenge 18 / 25 posters at bars.
- Keep a Refusals Log, record every time you refuse a sale due to age, intoxication, or disorderly behaviour.
- Train all staff / volunteers on licence rules and Challenge policy.

DON'T

- Serve anyone under 18 (unless the law or your license allows, e.g: 16–17 year-olds drinking beer, wine, or cider with a meal and accompanied by an adult, in certain premises).
- Serve someone who's drunk or buy alcohol for someone who is drunk (offence for both parties).
- Let unaccompanied under-18s into areas restricted by your licence.

4. If in Doubt – Don't Serve

- If the customer refuses to show ID or you're not sure it's genuine, refuse the sale.
- Always back up your staff's decision to refuse, your licence depends on it.

Build Phase

Construction and fit-out:

- Mark out and set up the site, structures, power, water, signage, and test systems before opening.

Site rules

- Especially useful during build and breakdown phases to ensure contractors are fully aware of restrictions and behave appropriately
- Site rules can include prohibited items, use and access of vehicles, speed limits, smoking, hours of operation etc.

Staffing & Workforce

- All staff and contractors vetted (DBS checks where required, right-to-work documentation)
- Induction and training completed: health & safety, emergency procedures, role-specific skills
- Training and awareness (e.g: ACT Awareness).
- Readiness and Drills
- Uniforms / PPE issued and correct
- Volunteer roles filled, briefed, and insured

Operational & Safety Readiness

- Pre-event staff briefing
- Draft Compliance Audit Checklist (see DSC Draft Compliance Audit Template below)
- Evacuation, Lockdown and Invacuation / Shelter plans in place

- Communications Plans in place
- Contacts lists and escalation pathways
- Information Sharing Agreement in place (for Mutual Aid and Incident Response Collaboration)
- Emergency response plan confirmed: contacts, communications plan and protocols, escalation triggers
- Site Safety File including:
 - Contractor RAMS (Risk Assessments and Method Statements) received and approved
 - Insurance documentation all in order (and max liability values checked)
 - Adverse Weather plan
 - Structures sign-offs
- Staff welfare provisions in place, breaks rota, catering, welfare facilities
- Where applicable attend a “No Objections” meeting facilitated by Local Authority hosting a final Safety Advisory Group (SAG) with required documentation

Run Phase

Public in attendance:

- The live event; manage operations, safety, and audience experience in real time.

Final Checks before gates open

(All items must be signed off before public access)

- ☐ Potable Water – supply approved, connections safe, points labelled, quality test on file.
- ☐ Power (Mains / Generator) – installed by competent person, certified, load capacity confirmed, isolation points marked.
- ☐ Sanitation & Toilets – adequate provision for capacity, accessible units in place, servicing contract active.
- ☐ Fire Safety – extinguishers in place and tested, correct types for risks, fire exits unobstructed.
- ☐ First Aid & Medical Cover – trained staff on site, kits in date and stocked, ambulance access clear.
- ☐ Structural Safety – temporary structures signed off by competent person with certificate.
- ☐ Emergency Lighting – operational and tested where required.
- ☐ Communications – radios or mobiles phones functional (note - coverage and performance may be affected by the surge in numbers at the site), contact lists issued to key staff.
- ☐ Stewards and Security Deployment – positions staffed, decision making authority / control point operational, access control active.
- ☐ Staff briefed – see [below](#).

- ☐ Waste & Litter Control – bins deployed, hazardous waste arrangements confirmed.
- ☐ Site inspection complete: hazards removed, signage in place, access routes clear.

Breakdown Phase and review

De-rig, restoration:

- Take down structures, pack away kit, clear waste, and return the site as agreed.
- Review what went well, poorly – learnings for next time.

Post-Event Checklist

(To be completed before final sign-off and site hand-back)

- Breakdown schedule briefed to staff and contractors.
- Site rules in force during the breakdown phase.
- Site cleared of spills, litter and waste, recycling completed; waste contractor sign-off obtained.
- Temporary structures dismantled and removed.
- Hot debrief held with key staff and contractors before they leave the site.
- All equipment and hired assets returned, including plant and machinery, with condition and fuel state checked (where applicable).
- Road closures and traffic management measures lifted, temporary signage removed.
- Site hand-back with condition check / dilapidations agreed.
- Staff and contractor sign-out completed, payroll / expenses processed – where applicable.
- Incident reports and near-miss logs collected and filed on Incident Management System.
- Feedback gathered from staff, volunteers, vendors and key stakeholders.
- Post-event report produced: including attendance, incidents, lessons learned.
- Follow up on any customer complaints or feedback.

6. Incident Reporting Template



Purpose: Record and analyse security incidents to improve future preparedness



Key Fields:

- **Incident specifics:**



Date:



Time:



Time stood down:

- **Location Details:** Where the incident occurred within the venue or event

- **Suggested Incident Categories:**

- ① 1 Fire
- ② 2 Security
- ③ 3 Crowd
- ④ 4 Venue
- ⑤ 5 Medical
- ⑥ 6 Lost Persons
- ⑦ 7 Information Security
- ⑧ 8 Property Damage
- ⑨ 9 Crime
- ⑩ 10 Near Miss
- ⑪ 11 Unspecified / TBC
 - **Decisions / Actions Taken:** Immediate responses and resolutions
 - **Support needed**
 - **Observations & evidence**
 - **Witnesses:**
 - ① Names
 - ② Contact details
 - **Attachments:** Yes/No
 - **Post-Incident Review:** Recommendations for preventing recurrence

7. Staff Briefing Checklist

- **Purpose:** To ensure that all event staff are fully briefed on operational roles, safety procedures and emergency protocols before the event begins.

- ① **Key Fields:**

- **1. General Event Information**

- ① Event name, date and location.
- ② Key event timings (doors open, peak periods, closing time).
- ③ Expected attendance numbers and crowd dynamics.
- ④ Event history including attendance and issues
- ⑤ Event layout, including entrances, exits, key areas (stage, VIP, first aid, etc.).
- ⑥ Event objectives and key stakeholders (organisers, security, contractors).
- ⑦ Sale and distribution of Alcohol and licencing matters.

- **2. Staff Roles & Responsibilities**

-  Individual responsibilities and reporting lines.
-  Responsible Person & chain of command and escalation procedures (use of control room if applicable).
-  Designated Premises Supervisor (DPS) for alcohol and licencing matters.
-  Check-in and check-out procedures.
-  Non-attendance and sickness of staff.
-  Code of conduct and customer service expectations.
-  Handling lost property and customer enquiries.
- **3. Health & Safety Procedures**
 -  Location of first aid stations and medical support.
 -  Identification of first aiders and designated safety officers.
 -  Fire safety procedures and fire assembly points.
 -  Crowd management protocols and safe capacities.
 -  Heat stress and hydration reminders (for outdoor events).
 -  Manual handling and lifting precautions.
 -  Food hygiene protocols.
 -  Permits to Work.
 -  Vehicles and speed limits.
 -  Vulnerable or Lost Persons Procedures
- **4. Security & Incident Response**
 -  Entry procedures, ticketing (including ticket types) and accreditation checks.
 -  Re-entry procedures (if any).
 -  Prohibited items, bag search policies and actions on finding same.
 -  Identification of security staff and stewards.
 -  Emergency evacuation routes and procedures.
 -  Responding to medical emergencies and security incidents.
 -  Suspicious packages and hostile reconnaissance awareness.
 -  Communication channels and radio call signs.
 -  Incident management and reporting / record keeping.
- **5. Emergency Procedures**
 -  Alarm signals and emergency PA announcements.
 -  Shelter-in-place and lockdown procedures (if applicable).
 -  Lost or vulnerable person protocol.

- Severe weather action plan (for outdoor events).
 - Coordination with emergency services (fire, police, ambulance).
 - Entry and escort of emergency vehicles.
 - Assembly points and evacuation leadership roles.
 - **6. Communication & Briefing Confirmation**
 - Radio distribution and check-in.
 - Team WhatsApp or SMS text alert groups (if used).
 - Contact details for supervisors and key personnel.
 - Dealing with the Press or Media.
 - **7. Round-up**
 - Confirmation of briefing understanding (staff sign-off or roll call).
 - Any last-minute updates or reminders.
 - **Sign-Off Confirmation**
 - Attendance sheet and or confirmation staff have received the briefing and understand their responsibilities.

8. Suspicious Item Reporting Form

- **Purpose:** To ensure an accurate record is made should an item be found.
- **Include:**
 - **Incident Details**
 - Date:
 - Time:
 - Location of Suspicious Item:
 - Reporting Staff Name:
 - Position/Role:
 - **Description of Suspicious Item**

Use the HOT principles:

 - **H – Hidden:** Is the item concealed or not obviously visible in a place where it shouldn't normally be?
 - **O – Obviously Suspicious:** Does the item look unusual for its environment? Does it have wires, tape, or odd smells, or is it leaking?
 - **T – Typical for the area?** Is the item unusual for that location? Would it normally be expected to be found there?
 - Size (Approximate Dimensions):
 - Shape: Box / Bag / Cylinder / Other:
 - Colour:
 - Material (Plastic, Metal, Fabric, etc.):
 - Any markings, labels, or writing on the item?
 - If yes, describe:

- Sounds or unusual smells?
- If yes, describe:

● **Discovery & Actions Taken**

- How was the item found?
- Who was present when the item was found?
- Was the area evacuated?
- Has security been informed?
- If yes, name of security officer informed:
- Have emergency services been contacted?
- If yes, time of contact:
- Name of responding officer (if applicable):
- Was the item moved or disturbed before reporting?
- If yes, explain:

● **Additional Observations**

- Was anyone seen placing or abandoning the item?
- If yes, description of person(s):
- Any suspicious behaviour in the area prior to discovery?
- If yes, details:
- CCTV coverage of the area?
- If yes, has security reviewed footage?

● **Reporting & Follow-Up**

- Reported to: Security / Event Control / Police / Other:
- Time of Report:

● **Actions Taken Post-Reporting:**

- Area Secured
- Awaiting Emergency Response
- Public/Staff Notified
- Other:

● **Sign-Off Confirmation**

- Reporting Staff Signature:

Instructions to staff:

- Do not touch or move the suspicious item.
- Refer to the Suspicious Item topic in the DSC Incident Response Playbook
- Keep people away from the area and follow evacuation protocols if necessary.
- Contact security or emergency services immediately.
- Record all details as accurately as possible to assist responders.

9. GDPR Compliance Guidance

- **Purpose:** Ensure all data collection, storage and sharing complies with data protection laws see <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/>
- **Include:**
 - Privacy notices for attendees and staff
 - Consent forms for data collection
 - Records of how personal data is stored, secured, amended and deleted

10. Document Storage and Sharing Guidelines

- **Purpose:** Outline a framework for securely managing and sharing compliance documents
- **Guidelines Include:**
 - Digital tools (e.g: cloud-based storage with encryption)
 - Access control lists for sensitive files (e.g: risk assessments)
 - Backup and recovery procedures for key documents
 - What documents need to be available to share, printed and / or on-line
Eg: Insurance, Public Protection Procedures / Security Plan, Site Safety File etc.

11. Annual Review

- **Purpose:** Ensure that all policies, procedures and documents are regularly updated
- **Checklist should include:**
 - Review of risk assessments to reflect new threats or changes to the venue
 - Update of emergency plans based on recent incidents or feedback
 - Verify training records for new or lapsed certifications
 - Update and confirm contact lists
 - Confirm insurance requirements (eg: level of cover and validity period)
 - Update National Events Database see [Link](#)

12. Optional: Public-Facing Policies

- **Purpose:** Build trust with attendees by sharing safety commitments
- **Examples:**
 - An abbreviated version of the security policy posted on the venue's website
 - Advice and instructions for attendees on what to do in emergencies

PART 17 - Directors and Officers Insurance: Protecting Decision-Makers

Purpose:

Directors and Officers Insurance (D&O) provides liability protection for individuals in leadership roles, including officers, directors and key decision-makers such as the **Responsible Person**. This coverage safeguards personal assets in the event of legal actions arising from their organisational responsibilities.

Key Benefits



Provides peace of mind to directors and officers, ensuring they are not personally exposed to financial or legal risks.



Underwrites organisational liability.



Reinforces organisational resilience by safeguarding key leadership against unforeseen claims.

Why D&O Insurance Is Relevant

(subject to guidance from the Home Office)



Legal Accountability:

- Under Martyn's Law, the **Responsible Person** may face legal scrutiny for non-compliance with security obligations.
- D&O Insurance covers defence costs, settlements, or judgments in case of legal claims alleging negligence or failure to fulfil compliance responsibilities.



Risk Management for Leadership:

- Organisations may hold directors and officers personally liable for errors or omissions in implementing security measures.
- Insurance protects these individuals, allowing them to execute their roles confidently.



Reputational Protection:

- Coverage extends to managing reputational risks associated with legal claims, ensuring the organisation and its leadership maintain trust among stakeholders.

Key Features of D&O Insurance



Coverage for Compliance Risks:

- Legal claims related to inadequate security planning or risk assessments.
- Allegations of failing to meet regulatory requirements under Martyn's Law.

Defence Costs and Settlements:

- Legal expenses for defending against claims of negligence.
- Payment of settlements or judgments related to covered claims.

Coverage for Civil and Regulatory Actions:

- Protection against fines or sanctions imposed by regulators such as the Security Industry Authority (SIA), if legally insurable.

Additional Protections:

- Covers employment-related claims, such as wrongful termination or discrimination, if connected to compliance duties.
- Offers crisis management support for reputational repair after incidents.

How to Include D&O Insurance in Compliance Planning

Review Current Policies:

- Ensure the organisation's existing D&O policy explicitly covers risks associated with your activities.

Discuss with Insurers:

- Engage with insurers to clarify how Martyn's Law-related risks are handled and ensure comprehensive coverage.
- Consider policies offered by specialists like **Pool Re**, who are active in terrorism risk management.

Provide Training for Directors:

- Include Martyn's Law obligations in D&O onboarding and training to reduce exposure to claims.

Document Risk Management:

- Maintain detailed records of risk assessments, security measures and compliance efforts to demonstrate diligence in case of claims.

D&O Insurance Checklist:

To evaluate and secure appropriate D&O coverage - key questions to ask insurers, such as:

- Does the policy cover terrorism related risks?
- Are fines or penalties insurable under the policy?
- What exclusions apply?

Sample Risk Disclosure Statement:

- For directors to disclose potential risks to the organisation's insurer, ensuring transparency

Case Studies:

- Look up examples of how D&O insurance has protected organisations and leadership in similar regulatory environments

**Educational Resources:**

- Webinars or guides are available from providers like **Pool Re** or major insurers on managing leadership risks under new regulations. See <https://www.poolre.co.uk/>

PART 18 - Primacy

What Is Primacy?

**Definition:**

- Primacy refers to the formal assumption of control over an incident by the Police or a Government Agency when the situation requires specialised expertise, resources, or legal authority.
- Examples include terrorism, public disorder, or major public safety threats
- Use the Memorandum of Understanding at [Appendix A](#) to establish roles and responsibilities

**When It Happens:**

- The Police or Government Agencies may assume primacy when:
 - A criminal act, such as a terrorist attack, is suspected
 - Public safety or national security becomes the overriding concern
 - Their resources or coordination are critical for effective management

What to Do When Primacy Is Transferred

**Acknowledge the Transition:**

- Document who has control at what point and when and who it was handed over to.
- Recognise the shift in control and defer decision-making to the lead authority
- Communicate this change to all staff and attendees if appropriate
- Use the Primacy Document (see [Appendix B](#) & [Appendix C](#) below) to formally hand over / return control

**Provide Full Cooperation:**

- Designate a senior representative (e.g: the Responsible Person) to liaise with the Police or Government Agency
- Share all relevant information, such as:
 - Risk assessments
 - Security plans
 - Incident details (e.g: times, locations and individuals involved)

**Follow Instructions:**

- Comply promptly with directions from the authorities
- Ensure staff and volunteers remain informed and coordinated to support their efforts

 Maintain Internal Operations:

- Continue managing non-critical aspects of the venue or event, such as attendee welfare and logistical support, as directed

Actions While the Police or Government Agency Has Control

 Staff and Volunteer Roles:

- Reassign staff to support roles as directed by the authorities (e.g: assisting with crowd management or providing access to restricted areas)
- Keep non-essential personnel away from operational zones to avoid interference

 Communication Protocols:

- Designate a single point of contact (POC) for the authorities to ensure streamlined communication
- ***Do not release independent statements to the media; defer all public communications to the authorities unless instructed otherwise***

 Safety and Welfare:

- Focus on the safety and welfare of attendees and staff by ensuring clear evacuation routes, first aid availability and emotional support if required

 Document Observations:

- Record actions taken by your organisation during the incident to assist with post-incident reviews and legal requirements

What to Do When Control Is Handed Back

 Reassess the Situation:

- Document who has control at what point and when and who it was handed over to
- Conduct a briefing with the authorities to understand the current status of the incident and any residual risks
- Review the condition of the venue or event site to ensure it is safe and desirable to resume operations

 Resume Responsibilities:

- Gradually take back control of operations under the guidance of the authorities
- Ensure all staff are re-briefed on their roles and the updated situation

 Post-Incident Review:

- Collaborate with the authorities to conduct a debrief, incorporating their feedback into your organisation's response plans

- Update your Incident Response Playbook based on lessons identified

Key Considerations

1. **Stay Flexible:**

- Be prepared to adapt your plans to align with the priorities of the Police or Government Agency

2. **Maintain Transparency:**

- Provide accurate and timely information to ensure the authorities can make informed decisions

3. **Prioritise Safety:**

- Keep attendees and staff informed and reassured while following all instructions from the authorities

Supporting Tools

• **Checklist for Handing Over Primacy:**

- Use the Memorandum of Understanding at [Appendix A](#)
- Use the Primacy transfer document at [Appendix B](#)
- Include contact details, risk assessment documents and other key information

• **Briefing Templates for Staff:**

- Prepare staff for the transition and their supporting roles

• **Checklist for Handing Back Primacy:**

- Use the Primacy transfer document at [Appendix C](#)
- Take contact details from the Police or Government Agency and other key information

• **Post-Incident Debrief Forms:**

- Capture key insights and recommendations from the authority-led response (or multi-agency response)

PART 19 - The legal bit: Decision Support Centre (DSC) & National Events Database (NED) Disclaimers

This Toolkit and associated resources, including the Incident Response Playbook and Responsible Persons Training materials, are provided for guidance only.

They are intended to support venues, events and organisations in developing a practical approach to preparedness, decision-making and incident response in real-world environments.

They do not constitute legal, professional or specialist advice, and should not be relied upon as a substitute for appropriate professional consultation where required.

While these resources have been developed with reference to current legislation and guidance, including the Terrorism (Protection of Premises) Act 2025 (Martyn's Law), they are not intended to provide definitive interpretation of legal obligations or regulatory requirements.

Users are responsible for ensuring that their approach reflects their specific circumstances, including the nature, scale and complexity of their venue or event.

No two environments are the same, and incidents may develop in ways that are dynamic, unpredictable and influenced by factors beyond immediate control. As such, the guidance provided should be applied with judgement and adapted as necessary.

The Decision Support Centre accepts no liability for any loss, damage or consequence arising from the use of, or reliance upon, these materials.

1. General Disclaimer

The Decision Support Centre (DSC) and National Events Database (NED) provide toolkits, playbooks and resources for informational purposes only. These materials do not constitute professional, legal, or regulatory advice. Users are encouraged to consult relevant experts (e.g: legal advisors, safety consultants) and ensure compliance with applicable laws, regulations and guidance (e.g: Terrorism (Protection of Premises) Act 2025, Health and Safety Act 1974, GDPR). The DSC and NED make no warranties or guarantees as to the accuracy, completeness, or applicability of these materials in specific circumstances.

The National Events Database is designed to support visibility across the events and venues ecosystem by providing a shared industry reference. It is intended to be a resource that may be useful to organisers, authorities, insurers and industry stakeholders and does not imply formal data sharing agreements.

References to third-party organisations and resources are provided for information purposes only and do not imply endorsement, partnership or formal affiliation.

2. Limitation of Liability

The DSC and NED are not liable for any direct, indirect, incidental, consequential, or other damages arising from the use or misuse of the materials provided. Users assume full responsibility for implementing safety procedures, risk management plans and incident responses based on their individual circumstances and requirements.

3. No Guarantee of Outcomes

While every effort has been made to ensure the resources provided are practical and accurate, the DSC and NED cannot guarantee that the implementation of these materials will prevent incidents, injuries, or legal compliance failures. Users must apply their own judgement, adapt procedures as necessary and consult professionals where required.

4. User Responsibility

It is the sole responsibility of users to assess the relevance, suitability and implementation of the materials provided within their own operations, venues, or events. The DSC and NED are not responsible for verifying individual safety measures, risk assessments, or legal compliance obligations.

5. Third-Party Links or References

The toolkits and playbooks may include references to third-party resources or websites. The DSC and NED do not control, endorse, or take responsibility for the accuracy, completeness, or availability of third-party content. Users access such resources at their own discretion.

Mention of a third party is for explanatory context only and does not imply any existing contractual, operational, or data sharing relationship.

However, we encourage organisers and venues to make use of publicly available guidance and training resources. Useful publicly available resources include ACT Awareness e-learning available through ProtectUK.

6. Intellectual Property Disclaimer

All content, including text, diagrams, templates and resources within the toolkits and playbooks, is the intellectual property of the Decision Support Centre (DSC) unless otherwise stated. Users may reproduce and use the materials for non-commercial purposes within their own venues or events. Unauthorised reproduction, modification, or distribution of these materials without prior written consent from the DSC is strictly prohibited.

7. Compliance with Regulations

The resources provided are intended to support venues and event organisers in implementing reasonable safety measures and best practices. Users must independently ensure compliance with relevant laws, regulations and guidance, including but not limited to the Health and Safety at Work Act 1974, Terrorism (Protection of Premises) Act 2025 (Martyn's Law) and GDPR obligations.

8. Tailored Solutions Disclaimer

The toolkits and playbooks provide general guidance and templates for managing incidents, safety and compliance. These resources are not specific to any individual

venue or event. Users must adapt and tailor the materials to meet their unique needs, risk profiles and operational requirements.



Appendices:



APPENDIX A - MEMORANDUM OF UNDERSTANDING

BETWEEN..... (COMPANY) AND ITS AUTHORISED
FUNCTIONARIES

AND

Venue / Event:

.....

Date:.....

This document should be read in conjunction with emergency procedures and incident management plans and though not legally binding it acknowledges that (company) and (borough or county) Police will work together in relation to this event and defines the respective functions and division of roles and responsibilities.

Company:

-  Will make provision for Health & Safety
-  (company) will make applications for and ensure compliance with, the premises licence
-  (company) will make provision of public safety for spectators, workforce and artists
-  (company) will ensure compliance with regulations in force at the time including maintenance of necessary licenses
-  (company) will make provision for stewarding and security, to ensure sufficient appropriately trained personnel on each location
-  (company) will be responsible for coordination of traffic management arrangements
-  (company) will provide the appropriate initial response to incidents
-  (company) will provide an up to date approved contingency plan compatible with the (company) emergency plan
-  (company) will be responsible for integrity of sportsmen and women, artists and backstage
-  (company) will provide command and control facilities in accordance with all appropriate legislation and guidelines
-  (company) will appoint and deploy safety officers
-  (company) will in partnership with other statutory authorities provide an appropriate resource to meet their responsibilities between transport hubs and venue

Police:

-  Protect life and property and respond to any threat to life
-  Maintain public order
-  Prevent, detect and respond to crime
-  Take control from (company) of a crowd management situation where they perceive that there is an impending threat to life
-  In partnership with (company) and other statutory authorities provide appropriate resource to meet their responsibilities between transport hub and venue
-  Provide a response to any breaches of the traffic management arrangements and/or disorder arising from them
-  Appoint and provide a 'Bronze' commander
-  Provide an emergency plan compatible with (company) contingency plan

Transfer of Primacy

Where there is a serious concern for public safety within the event site and the Police / Government Agency commander decides by virtue of his or her duty to preserve life and protect property, that it is necessary to take overall control of public safety, he or she will assume responsibility together with primacy of control for all or part of the event site and surrounding area.

In any circumstances where the duty Police / Government Agency commander decides or agrees with a request from the event promoter or his/her nominated representative, that he or she has to take overall control of all safety and public order aspects at any or part of the event by virtue of his or her duty to preserve life and protect property, he or she shall consult or notify the event promoter or his/her nominated representative of that decision.

During this period of Police / Government Agency primacy, the employees and agents of the (company) will work in conjunction with and under the direction of the Police commander.

Such transfer will be recorded in writing by completion of the primary document (see appendix A) as soon as practicable retrospective written agreement must be completed at the earliest opportunity, clearly defining the parameters of such handover.

During any period where Police / Government Agency has taken primacy of the event or crime scene, Police / Government Agency will also take primacy in addressing the media in relation to that incident.

When a situation exists where the Police / Government Agency commander decides that Police / Government Agency primacy is no longer necessary, the divisions of responsibility will revert to those outlined in the preceding sections. Return to normality will be carried out in consultation with event promoter or nominated representative and be confirmed in writing (see appendix A below).

Variations

Any variations as to the division of responsibility MUST be agreed in writing between the event promoter and Police / Government Agency and will be appended to this document.

Signed

Name Role
On behalf of (company)

Date

Signed

Name Rank

On behalf of (Police / Government Agency)

Date

APPENDIX B – TRANSFER OF PRIMACY TO POLICE OR GOVERNMENT AGENCY – DOC 1 of 2

(Borough or County) Police PRIMACY DOCUMENT

Transfer of Primacy to Police / Government Agency

I as Police / Government Agency Commander

For (Specify the event)

 Being satisfied an incident has reached a critical stage and is beyond the capacity of the event promoter or his/her nominated representative to address and/or having been notified by event promoter or his/her nominated representative that this is the case;

 or due to a serious concern for public safety

 or a Major incident has already been declared by Rank (name and rank of person declaring Major incident)

 at the specific request of the event promoter or his/her nominated representative (name of authorised individual)

 or by joint agreement between Police / Government Agency (name and rank) and event promoter or his/her nominated representative (name of individual)

 or my sole decision (name and rank)

I take primacy and control of operations within the event/part of/and/or its environs

Location (specify location of transfer)

Signed

Name Rank

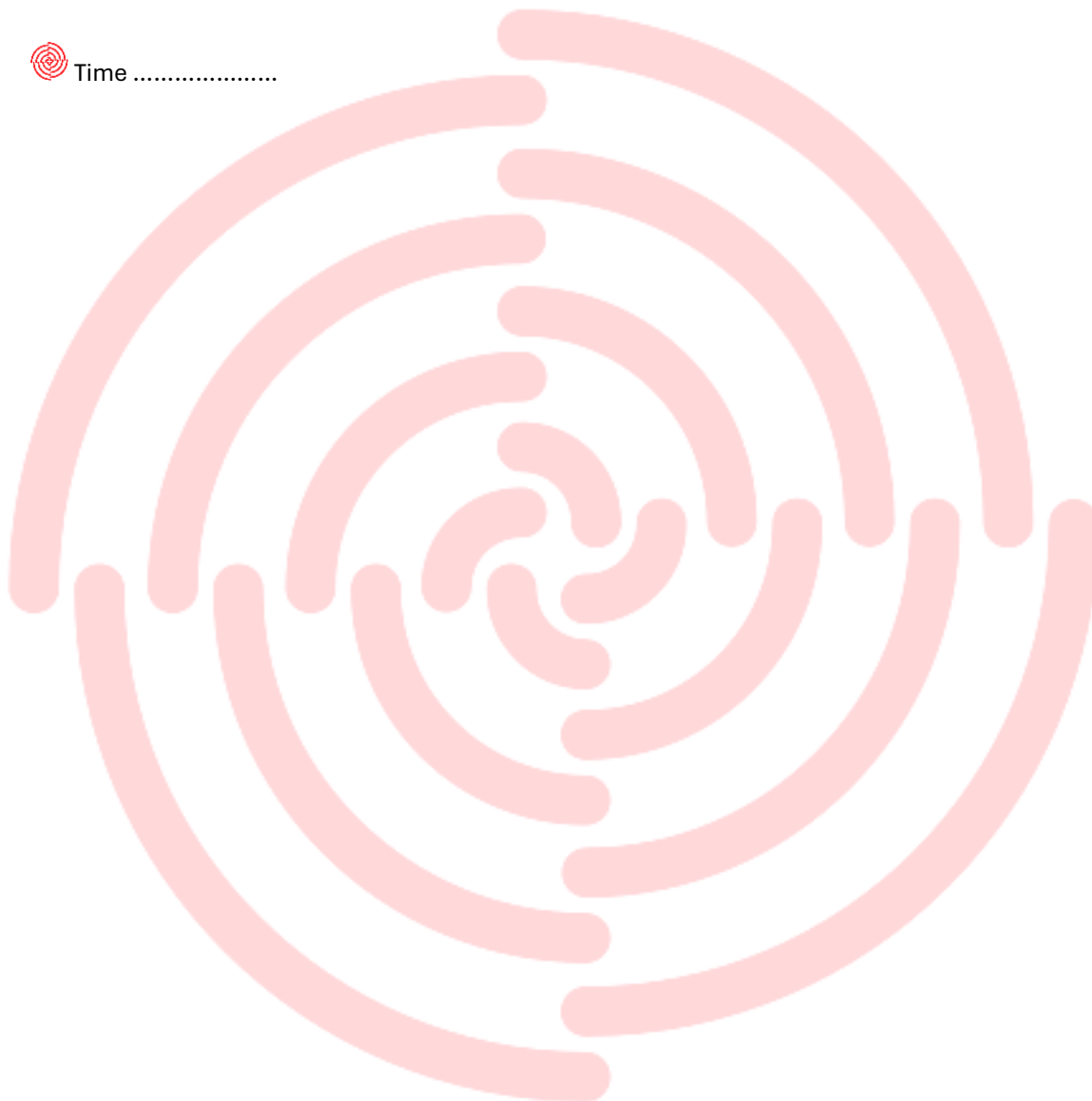
Police / Government Agency Commander

Signed

Name Position
Event promoter or nominated representative

 Date

 Time



APPENDIX C - TRANSFER OF PRIMACY FROM POLICE OR GOVERNMENT AGENCY – DOC 2 of 2

(Borough or County) Police PRIMACY DOCUMENT

Transfer of Primacy back to Event Promoter or Nominated Representative

I (Police / Government Agency commander

Being now satisfied that it is within the event management's capacity to safely continue operations and/or normality has been restored;

Hereby relinquish full responsibility for public safety and primacy and control back to the event promoter or his/her nominated representative.

Location (specify location of transfer)

Signed

Name Rank
Police / Government Agency Commander

Signed

Name Position
Event promoter or nominated representative

 Date

 Time

APPENDIX D - Information Sharing Agreement (ISA) Template

For Use in Mutual Aid and Incident Response Collaboration

1. Purpose of the Agreement

This Information Sharing Agreement sets out the lawful basis, principles and safeguards for the sharing of personal and operational data between the parties listed below for the purpose of mutual aid, incident response and collaborative safety and security planning.

2. Parties to the Agreement

This agreement is between the following organisations:

[Party A]

Organisation Name

Contact Name & Role

Contact Details

[Party B]

Organisation Name

Contact Name & Role

Contact Details

[Optional Parties]

Each party is a data controller for the personal data it holds.

3. Legal Basis for Sharing

Data will be shared under the following lawful basis as defined by Article 6 of the UK GDPR:

- a) Legal obligation: To comply with health and safety or public protection duties.
- b) Vital interests: To protect the life of an individual in an emergency.
- c) Public task: Performance of a task carried out in the public interest or official authority.

Where special category data is shared, the additional legal basis under Article 9 shall be:

- d) Substantial public interest under DPA 2018 Schedule 1, Part 2.

4. Data to Be Shared

Data may include (but is not limited to):

- Name and contact details of Responsible / Accountable Persons
- Incident logs or witness reports
- CCTV or body-worn video footage
- Emergency planning documentation
- Crowd risk information or safeguarding concerns

5. Information Sharing Principles

All parties agree to:

- Share only the minimum necessary data for the stated purpose
- Maintain accuracy and timeliness of shared data
- Apply appropriate security controls (encryption, access controls)
- Maintain records of what data was shared and when

6. Retention and Deletion

Each party will retain shared data only for as long as necessary to fulfil the agreed purpose, subject to their own retention schedules. Any onward sharing must be consistent with the original purpose.

7. Data Subject Rights

Where applicable, each party will respect the data rights of individuals under UK GDPR, including:

- The right to be informed
- The right of access
- The right to rectification or objection (subject to exemptions in emergencies)

8. Security Measures

Each organisation confirms it has appropriate technical and organisational measures in place to:

- Prevent unauthorised access, alteration, disclosure, or loss
- Ensure availability of data during emergency operations

9. Breach Notification

If a personal data breach occurs, the party discovering it must:

- Notify affected parties without undue delay
- Cooperate in containment and reporting
- Follow their own ICO reporting obligations

10. Review and Duration

This agreement is valid for a period of 12 months from the date of signing or until replaced. It will be reviewed:

- After any major incident
- If data protection law changes
- Annually, as part of preparedness planning

11. Signatories

Signed on behalf of [Party A]:

Name: _____

Role: _____

Date: _____

Signed on behalf of [Party B]:

Name: _____

Role: _____

Date: _____

Other parties:

Additional Notes:

- This template can be adapted for specific use cases (e.g: between local authority and venue, or multiple event partners).
- It can be attached to or referenced in Mutual Aid MOUs or Service Level Agreements.

APPENDIX E – DSC Readiness Review Template

Venue/Event Name: _____
 Tier Classification: ☐ Standard (200–799) ☐ Enhanced (800+)
 Responsible Person: _____
 Date of Audit: _____
 Auditor (if applicable): _____

Section 1: Legal Duties & Responsible Person

Criteria	Yes	No	Notes / Evidence
Responsible Person appointed	☐	☐	
Tier classification determined and documented	☐	☐	
Security Plan completed and reviewed within the last 12 mths	☐	☐	
Staff aware of their roles	☐	☐	

Section 2: Training and Awareness

Criteria	Yes	No	Notes / Evidence
All staff/volunteers have completed ACT e-learning	☐	☐	
Validation of Process (VoP) workshop (testing BAU)	☐	☐	
Briefings held before each public event	☐	☐	
Regular drills or scenario exercises undertaken	☐	☐	
Training records are documented and accessible	☐	☐	

Section 3: Risk Management and Mitigation

Criteria	Yes	No	Notes / Evidence
Terrorism risk assessment completed and appropriate to tier	☐	☐	
Risk mitigation measures are proportionate and in place	☐	☐	
Records maintained for all identified risks and actions taken	☐	☐	
HVM and access control measures	☐	☐	

Section 4: Emergency Response Planning

Criteria	Yes	No	Notes / Evidence
Lockdown, evacuation, and shelter-in-place procedures defined	☐	☐	
Emergency contacts up to date and accessible	☐	☐	
Public and media communication protocols prepared	☐	☐	
Plans tested via live or table-top exercise in last 12 months	☐	☐	

Section 5: Documentation and Review

Criteria	Yes	No	Notes / Evidence
Version control applied to the Security Plan	☐	☐	
Training records, incident logs, and debriefs stored centrally	☐	☐	
Last internal review completed within 6 months	☐	☐	
Security Plan Template used or equivalent structure followed	☐	☐	

Continued over../..

Section 6: Liaison and External Coordination

Criteria	Yes	No	Notes / Evidence
Contact made with CTSA or local police	☐	☐	
Event details shared with SAG or licensing body	☐	☐	
Roles for emergency services and authorities defined in plan	☐	☐	
Stakeholder communication protocols rehearsed	☐	☐	

Summary & Actions

Overall Status:

- ☐ Ready (SFARP)
- ☐ Minor Improvements Required
- ☐ Significant Improvements Required

Next Steps / Action Plan:

- 1.
- 2.
- 3.

Date for Next Review:

ACT Training records:

Name	Role	Date taken
------	------	------------

APPENDIX F - DSC Validation of Process (VoP) Workshop Template

Purpose

The Validation of Process (VoP) workshop is designed to test how your event or venue operates under normal conditions (Business as Usual – BAU), before introducing incident scenarios.

It helps identify how effectively:

- information flows
- decisions are made
- teams coordinate
- responsibilities are understood

Key Principle

Effective incident response depends on effective day-to-day operations.

1. Workshop Overview

Event / Venue

Date

Facilitator

Attendees

Phase (Planning / Build / Live / Breakdown)

BAU Process Validation

2. Workshop Objectives

Tick or define focus areas:

- ☐ Validate communication pathways
- ☐ Confirm roles and responsibilities
- ☐ Test decision-making flow
- ☐ Review coordination between teams
- ☐ Assess situational awareness (COP)
- ☐ Identify gaps or friction points

3. Scenario Context - BAU Only (This is not testing an incident scenario; this is testing normal operations.)

Describe a typical operating period, for example:

- Build phase with contractors active
- Event open to public (peak period)

- Multi-agency presence (security, medical, operations)

4. Process Mapping (Live Walkthrough)

Facilitator to guide discussion:

A. Information Flow

- How is information received?
- Who needs to know?
- Who receives it first?
- How and when is it shared?
- Is there a natural hand-off?
- For something to proceed does another action need to precede it?

B. Decision-Making

- Who makes decisions at each stage?
- What information informs those decisions?
- Are decisions recorded?

C. Communication Channels

- Radios / digital platforms / face-to-face
- Primary vs fallback methods
- Clarity and consistency

D. Roles & Responsibilities

- Are roles clearly understood?
- Any overlaps or gaps?
- Any confusion in authority vs responsibility?

E. External Interfaces

- Emergency services
- Local Authority / SAG
- Contractors / suppliers

5. Control & Coordination Check

Use this section to explore alignment:

Area Observations

Who appears to hold operational control?

Is control clear or fragmented?

How is coordination achieved?

Are there delays or bottlenecks?

6. Situational Awareness (COP)

- Do all teams share the same understanding of what is happening?
- Is there a recognised “single version of the truth”?
- How is information updated and verified?

7. Observations & Friction Points

Capture issues such as:

- Delayed communication
- Conflicting instructions
- Unclear escalation thresholds
- Over-reliance on individuals
- Gaps between teams

8. Actions & Improvements

Issue Identified	Action Required	Owner	Timeline
------------------	-----------------	-------	----------

9. Link to Scenario Testing

Following this workshop:

- ☐ Proceed to table-top exercise
- ☐ Update plans before further testing
- ☐ Conduct targeted training / briefings

Key Principle

Fix the system before testing the crisis.

10. Facilitator Notes (Optional)

- Keep discussion grounded in reality
- Avoid introducing artificial scenarios
- Focus on how things actually work, not how they are written
- Encourage honesty — this is not an audit, it is a learning process

APPENDIX G - DSC Safety Advisory Group Guidance (SAG / ESAG)

DETERMINING SAG APPLICABILITY

STEP 1 - QUESTION: IS THERE A DUTY TO ENGAGE EXTERNAL BODIES?

Ask:

Does the event create risks or impacts beyond the organiser's direct control?

If NO

- Low-risk, contained, routine activity
- No impact on highways, neighbours, emergency services
- Operates wholly under an existing premises licence or permission

Likely No SAG required

- Maintain normal liaison as appropriate
- Retain evidence of risk assessment

If YES

- Public safety implications
- Off-site or community impact
- Emergency response may be affected

Likely SAG required

Proceed to Step 2

STEP 2 - QUESTION: DO COMMON SAG TRIGGERS APPLY?

If One or more are "YES" a SAG / ESAG may be justified:

Event Scale & Profile

- Large attendance or high crowd density
- Camping
- Significant ingress / egress movements
- High media, political, or community sensitivity

Risk Complexity

- Alcohol-led event
- Counter-terrorism considerations
- Temporary structures (stages, marquees, grandstands)
- Adverse weather exposure
- Crowd dynamics not previously tested
- Known criminality

Location & Impact

- City centre / transport hub

- Road closures or traffic management
- Noise, environmental health, or residential impact
- Consequences of more than one event taking place in the locality
- Heritage / iconic / sensitive site

Organisational Factors

- Novel, new or materially changed event
- New organiser or delivery model
- Limited track record at the location

If ALL are NO - a SAG is usually disproportionate

If ANY are YES

Proceed to Step 3

STEP 3 - QUESTION: IS A SAG THE PROPORTIONATE MECHANISM?**Consider:**

Can risks be managed through:

- Licensing process?
- Normal operational liaison?
- A separate planning group?
- Existing multi-agency protocols?

If YES - a SAG likely adds no additional value. Risks are already well controlled

- Likely No SAG required
- Record rationale

If NO

- Multi-agency coordination needed
- Shared situational awareness required
- Early intervention reduces risk

A SAG / ESAG is appropriate

Proceed to Step 4

STEP 4 - HOW SHOULD THE ORGANISER RESPOND DURING A SAG?

(A sample draft agenda is included below)

Core Principles

- **Prepared:** Risk assessment, Event Management Plan, contingencies
- **Open:** Engage constructively
- **Bounded:** Understand SAG is *advisory*, not an approval body

In the Meeting

Clarify:

- Advice vs statutory requirements
- Licensing matters vs safety advice

Test proportionality:

- “What risk is this addressing?”
- “What evidence or standard supports this?”

Avoid scope creep:

- New issues → log, assess, respond separately

Action Points

- Agree only to: Proportionate, evidence-based actions
- Record: Who advised what and what the organiser will consider or implement
- Ensure accurate minutes

Leave with a clear, documented position

STEP 5 - POST-SAG ACTION

- Review advice internally
- Implement proportionate controls
- Document rationale where advice is not followed
- Maintain audit trail

SAG Etiquette Checklist for Event Organisers

This is not about compliance paperwork, it's about *how you show credibility, proportionality and control.*

Before the SAG Meeting

Attendees

- Consider who is a Core member and who may be an Invitee:

(A core member can be expected to attend all meetings, an invitee may only be involved in specific events, meetings or agenda items.)

- Core membership of a group is likely to include:
 - Event organisers / promoters
 - Police Service

- Fire and Rescue Service
- NHS Ambulance Service
- Licensing
- Health representatives
- Traffic / transport providers
- Highways Agency
- Invited members may include:
 - Local Public Health teams
 - Venue owner / operator
 - Stewarding / security
 - British Transport Police
 - Maritime and Coastguard Agency
 - Harbour Authorities
 - Medical / first aid providers
 - Resident / community representatives
 - Crowd safety managers
 - Building Authority
 - Environmental Health
 - Council Communications Team
 - Civil contingency unit

Preparation & Materials

- Event Management Plan (EMP) is current and coherent
- Risk Assessment(s) reflect(s): crowd, terrorism, weather, structures, alcohol (where applicable)
- Site plan is clear and version-controlled
- Emergency arrangements are realistic and tested
- Roles and responsibilities are explicitly defined

Governance & Authority

- Named decision-maker attends (or is formally represented)
- Clear understanding of:
 - what is licensed
 - what is advisory
 - what sits outside the organiser's control

Mindset

- Open to advice
- Clear on proportionality
- Ready to explain *why* controls are sufficient, not just *what* they are

During the SAG Meeting

Conduct & Engagement

- Listen actively and respectfully

- Avoid defensive or adversarial language
- Ask clarifying questions where advice is unclear

Boundary Management (Critical)

Politely distinguish between:

- Advice
- Statutory requirements
- Licensing conditions

Challenge scope creep constructively: e.g: “Can we clarify the risk this is intended to mitigate?”

Evidence-Led Discussion

Reference recognised guidance and standards where relevant

Explain how risks are:

- identified
- mitigated
- monitored
- escalated

Decision Discipline

Do **not** agree to actions:

- without clarity of legal basis
- without assessing proportionality

Ensure actions are framed as:

- “to be considered” unless legally required

Recording & Accountability

Accurate minutes requested and reviewed

Advice is clearly attributed (who advised what)

Actions include:

- owner
- rationale
- timescale

Disagreements or alternative approaches are recorded professionally

Consider whether the notes and minutes of SAG meetings should be published and therefore subject to the Freedom of Information Act.

After the SAG Meeting

Follow-Up

- Review advice internally
- Implement proportionate measures where appropriate
- Where advice is not followed:
 - document the rationale
 - reference evidence and risk assessment

Assurance

- Maintain an audit trail demonstrating:
 - cooperation
 - competence
 - decision-making discipline

SAG Etiquette Golden Rules

- **A SAG advises, it does not approve**
- **Professional challenge is expected**
- **Documentation protects both organiser and authorities**

Sample - Organiser-led SAG agenda:

Purpose:

- Agree goals, roles and boundaries at the top of the meeting
- Make risk ownership vs risk oversight visible and explicit
- Keep the SAG: **Risk-Led, Proportionate, Advisory**

Pre-Meeting Circulation

At least in draft, three months prior to the event taking place but at a minimum four weeks, or where major events are taking place 6 months lead time may be needed:

- Event overview (What / Where / When / Who)
- Event Management Plan (current version)
- Risk Assessment (including terrorism risk where applicable)
- Site plan(s)
- Previous SAG actions (if applicable)

Principle:

The meeting is for assurance and advice, not document discovery.

1. Welcome, Purpose & Governance (5 mins)

 Likely led by: Event Organiser / Responsible Person

1.1 Purpose of the SAG

Agree that the purpose of the meeting is to:

- Share situational awareness
- Test the organiser's risk logic
- Receive multi-agency advice
- Identify material gaps or dependencies

Explicitly confirm:

- The SAG is **advisory**
- The organiser **retains risk ownership**
- No approvals are being sought or given
- A quality assurance process is in place in terms of the safety arrangements for events

1.2 Roles & Responsibilities (The Constitution)

Role	Responsibility
Event Organiser / RP	Risk ownership, decision-making
SAG members	Risk oversight, advice, challenge
Local Authority	Convening / facilitation (not direction)
Emergency services	Response feasibility & interoperability advice

2. Agreement of Meeting Structure & Decision Boundaries (5 mins)

 Likely led by: Local Authority

Confirm and record the following distinctions:

2.1 Definitions (Agreed Once, Used Throughout)

- Risk Ownership - Decisions and controls implemented by the organiser.
- Risk Oversight - Independent scrutiny, challenge and advice provided by SAG members.
- Statutory Requirement - Must be complied with (clearly identified and referenced).

- Advisory Recommendation - To be considered proportionately by the organiser.

2.2 How Agenda Items Will Be Handled

For each agenda item:

- Organiser presents risk logic
- SAG members provide advice / challenge
- Distinction recorded between:
 - advice
 - requirements
 - follow-up actions

3. Event Overview & Risk Context (10 mins)

- Event concept and objectives
- Attendance profile and crowd dynamics
- Site and location sensitivities
- Operating hours and key phases

Risk Ownership: Organiser

Risk Oversight: SAG

Focus: Understanding *why* the event is designed the way it is, not redesigning it in the room.

4. Risk-Led Agenda Items (Core of the Meeting)

Each section follows the same discipline, reinforcing ownership and oversight.

4.1 Crowd Management & Movement

- Ingress / egress strategy
- Capacity assumptions
- Density controls
- Monitoring and escalation triggers

Risk ownership: Organiser

Risk oversight: Police / LA / Fire

4.2 Security & Counter-Terrorism Considerations

- Responsible Person
- Martyn's Law tier (if applicable)
- Threat context and risk assessment (as understood by organiser)
- Proportionate mitigations
- Procedures

- Stewarding / searching / hostile vehicle mitigation (if applicable)
- Communication and response arrangements
- Stakeholder mapping

Risk ownership: Organiser / Responsible Person

Risk oversight: Police (CT / local), LA

4.3 Emergency Response & Interoperability

- Incident command structure
- Emergency access and rendezvous points
- Casualty management assumptions
- Interface with emergency services

Risk ownership: Organiser

Risk oversight: Police / Fire / Ambulance

4.4 Temporary Structures & Site Safety

- Structures in use
- Design, inspection and weather triggers
- Load and occupancy assumptions

Risk ownership: Organiser / contractors

Risk oversight: LA / Fire / specialists

4.5 Environmental, Community & Infrastructure Impacts

- Noise
- Traffic management
- Neighbours and local stakeholders

Risk ownership: Organiser

Risk oversight: LA / Highways / EHO

5. Summary of Advice, Actions & Decisions (10 mins)

5.1 Advice Log (Live)

- Who advised
- On what issue
- Rationale

5.2 Organiser Response

- Accepted and implemented
- Accepted with modification
- Not adopted (with rationale)
- Or “to be considered” unless legally required

Important:

Recording a rationale is good governance, not resistance.

6. Confirmation of Outcomes & Next Steps (5 mins)

- Confirm:
 - Actions
 - Owners
 - Timescales
 - Confirm no implied approvals
- Confirm minutes will:
 - distinguish advice from requirements
 - reflect organiser ownership
 - Agree / confirm whether minutes will be formally published (be clear on what might be contained in a Freedom of Information (FOI) request)

7. Close

Suggested key closing statement:

“Thank you for your advice and challenge. The organiser will now review and respond proportionately, retaining responsibility for final decisions and delivery.”