Connect › Support › Advance

The Institute of Internal Auditors Australia

# Session 2A
## Event management, risk, security and the role of internal audit

*Presented by*

Craig Sheridan
Managing Director
Sheridan Consulting Group

The Institute of Internal Auditors Australia

# Event Management, Risk, Security and the role of internal audit

Craig Sheridan APM

Sheridan Consulting Group

SCG
sheridan consulting group

# Protecting Crowded Places

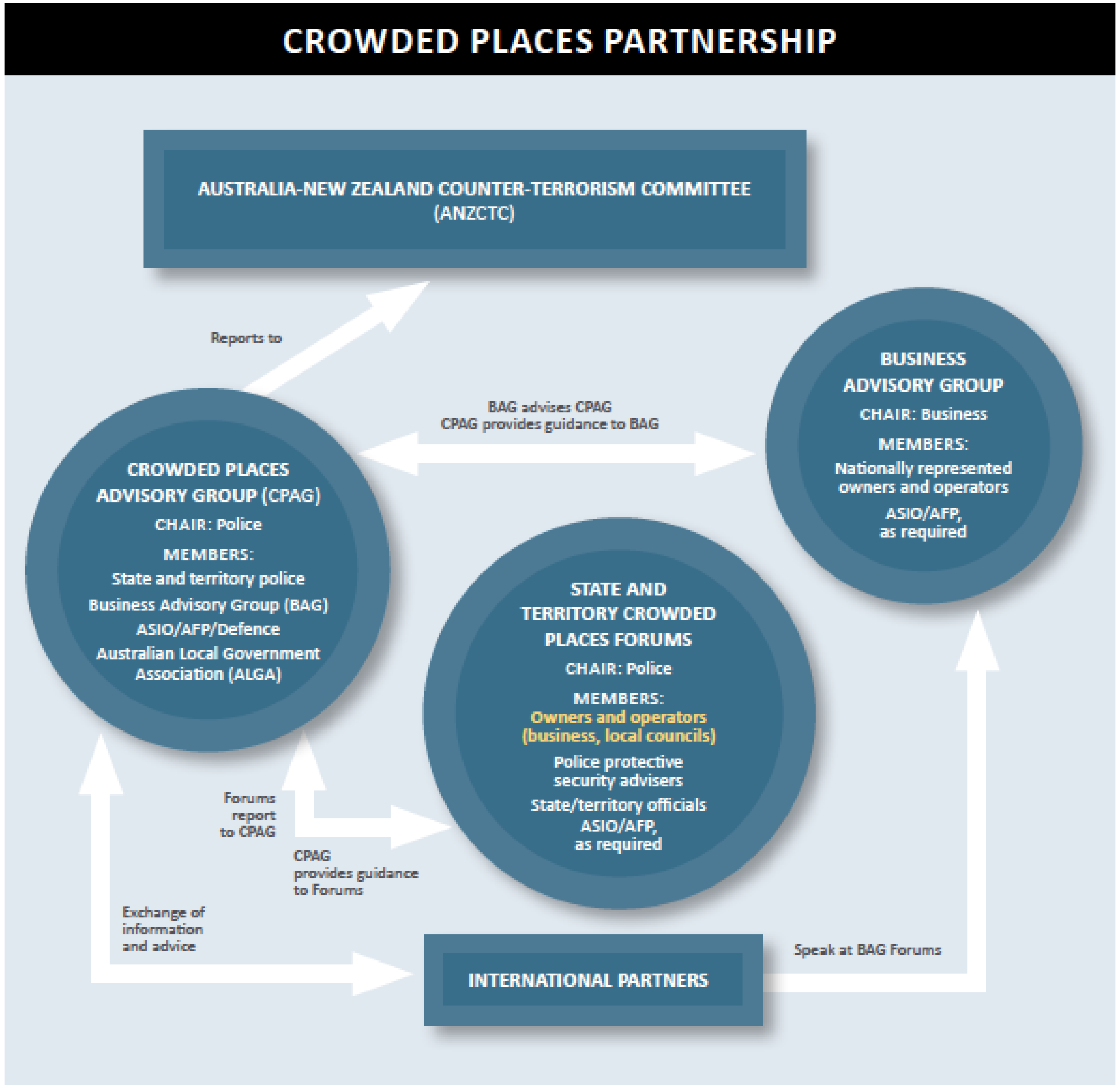
Objective – protect lives & make these spaces more resilient.

Success rests on strong partnerships between Governments and Private Sector

Four core elements;

1. Building Stronger Partnerships
2. Enabling better information Sharing and Guidance
3. Implementing Effective  Protective Security
4. Increasing Resilience

SCG
sheridan consulting group



# CROWDED PLACES PARTNERSHIP

AUSTRALIA-NEW ZEALAND COUNTER-TERRORISM COMMITTEE (ANZCTC)

Reports to

CROWDED PLACES ADVISORY GROUP (CPAG)
CHAIR: Police
MEMBERS:
State and territory police
Business Advisory Group (BAG)
ASIO/AFP/Defence
Australian Local Government Association (ALGA)

BAG advises CPAG
CPAG provides guidance to BAG

BUSINESS ADVISORY GROUP
CHAIR: Business
MEMBERS:
Nationally represented owners and operators
ASIO/AFP, as required

STATE AND TERRITORY CROWDED PLACES FORUMS
CHAIR: Police
MEMBERS:
Owners and operators (business, local councils)
Police protective security advisers
State/territory officials
ASIO/AFP, as required

Forums report to CPAG

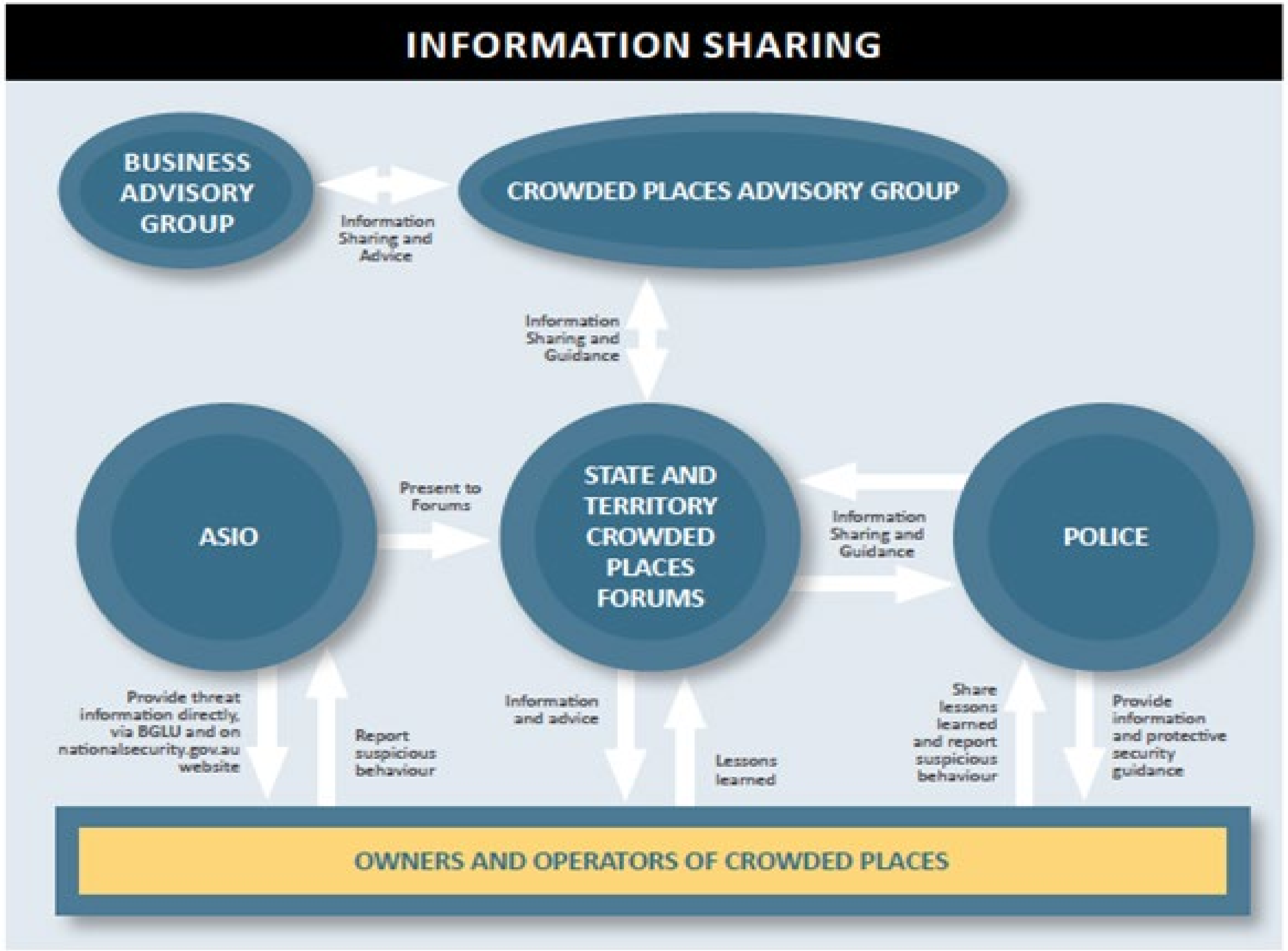
CPAG provides guidance to Forums

Exchange of information and advice

INTERNATIONAL PARTNERS

Speak at BAG Forums

Source: Figure 4 Crowded Places Partnership – Australia’s Strategy for Protecting Crowded Places from terrorism 2017.


INFORMATION SHARING
BUSINESS ADVISORY GROUP
Information Sharing and Advice
CROWDED PLACES ADVISORY GROUP
Information Sharing and Guidance
ASIO
Present to Forums
STATE AND TERRITORY CROWDED PLACES FORUMS
Information Sharing and Guidance
POLICE
Provide threat information directly, via BGLU and on nationalsecurity.gov.au website
Report suspicious behaviour
Information and advice
Lessons learned
Share lessons learned and report suspicious behaviour
Provide information and protective security guidance
OWNERS AND OPERATORS OF CROWDED PLACES

Source: Figure 5 Information Sharing – Australia's Strategy for Protecting Crowded Places from terrorism 2017.

# Australian Strategy – Who has a role?

Owners and operators of crowded places include;

- Major event organisers
- Sporting clubs
- Charities
- Community groups
- State, Territory and Commonwealth governments

# Australian Strategy – Responsibilities

Owner and Operators of Crowded Places responsibilities;

- Protecting their sites
- Duty of care to protect people
- Understand what the current threat environment means for security at their site
- **Undertake a risk assessment/ vulnerability analysis**
- Implement appropriate mitigations, **monitor and review**

# Event and Site Vulnerability Assessment

- Event / Organisation background
- National and local security environment awareness
- Site inspection & observation
- Protective security assessment
- Hostile vehicle vulnerability assessment
- Proposed mitigation strategies

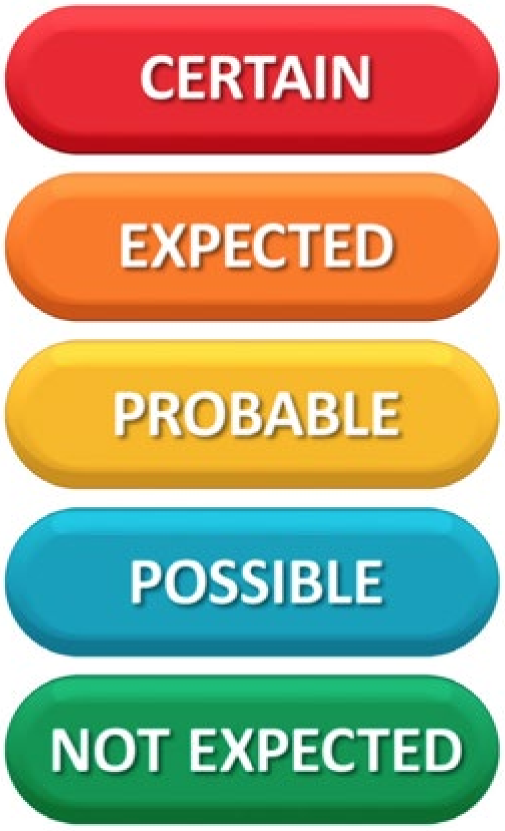
# Current Threat Environment

- Significant changes in the threat environment

- A growing responsibility for everyone in the community

- Patron safety and security is the major consideration for all crowded places

# National Threat Level



**PROBABLE –**

Individuals and groups continue to possess the intent and capability to conduct a terrorist attack in Australia. The elevated terrorist threat is likely to persist for the foreseeable future and it is not confined to any one city or metropolitan area.

# National Threat Level

ASIO considerations to lift the alert level;

- No. of Australians who hold violent extremists views has increased significantly with an intent to carry out violent acts.
- No. of Australians currently participating in conflicts overseas has increased significantly.
- No. of Australians who have returned from overseas after participating in these conflicts.
- No. of Australians who have been prevented from travelling overseas to participate

# Dominant Terrorist Attack Methods

### ARMED ACTIVE OFFENDER

Terrorist attack using firearms. Can range from pistols, shotguns to automatic assault rifles. These attacks have caused the greatest number of casualties.

### PERSONAL IED

Attacks utilising small IEDs that can be carried on an individual person such as a suicide vest or bomb carried in a backpack or other bags/luggage.

### VEHICLE RAMMING

Attack carried out by ramming vehicles ranging from cars to trucks and bulldozers into crowds.

### IMPROVISED WEAPON

Attacks carried out using improvised weapons and everyday objects including knives, axes and machetes.

# Attractive Targets for Terrorists

### PUBLIC PLACES

Sites targeted were all places which were open to the public such as museums, theatres, train stations, airports, and public streets.

### CROWDS

Sites targeted tended to attract large crowds due to their function or nature such as event venues or mass transit areas.

### EVENTS

Attacks also targeted special events including sporting events and events held on significant holidays.

### SYMBOLISM AND VALUE

Many of the sites targeted had some sort of symbolic value such as political symbolism (headquarters of agency or military memorial), cultural value (museum) functional value (airports and train stations) and critical infrastructure value (oil and gas, water, communications).

# Current Threat Environment

The changes in the security threat environment has forced changes in our approach to security planning, preparedness and response. We have moved away from;

- Reactive security procedures
- Low risk contraband detection
- Reactive management of crowd behaviour
- Temporary crowd control measures
- Basic access control to sites
- Basic reactive training of security guards

# Current Threat Environment

The changes in the security threat environment has moved our approach to;

- Increased levels of planning
- Increased levels of organisation and coordination
- High level of proactive detection and prevention – increased use of technology
- Permanent crowd management and asset protection principles
- Focused planning and response strategies on low capability high impact attacks
- Monitor and Review plans

# Owner/ Operator Responsibilities

- Understanding what the current threat environment means for security on site
- Protecting their sites
- Undertaking a risk assessment/ vulnerability analysis
- Implementing appropriate mitigations, monitor and review
- Adjusting security management plans in line with the threat level
- Raising awareness amongst staff and patrons
- Understanding main factors that influence terrorist target selection
- Reporting security incidents and suspicious activity to authorities

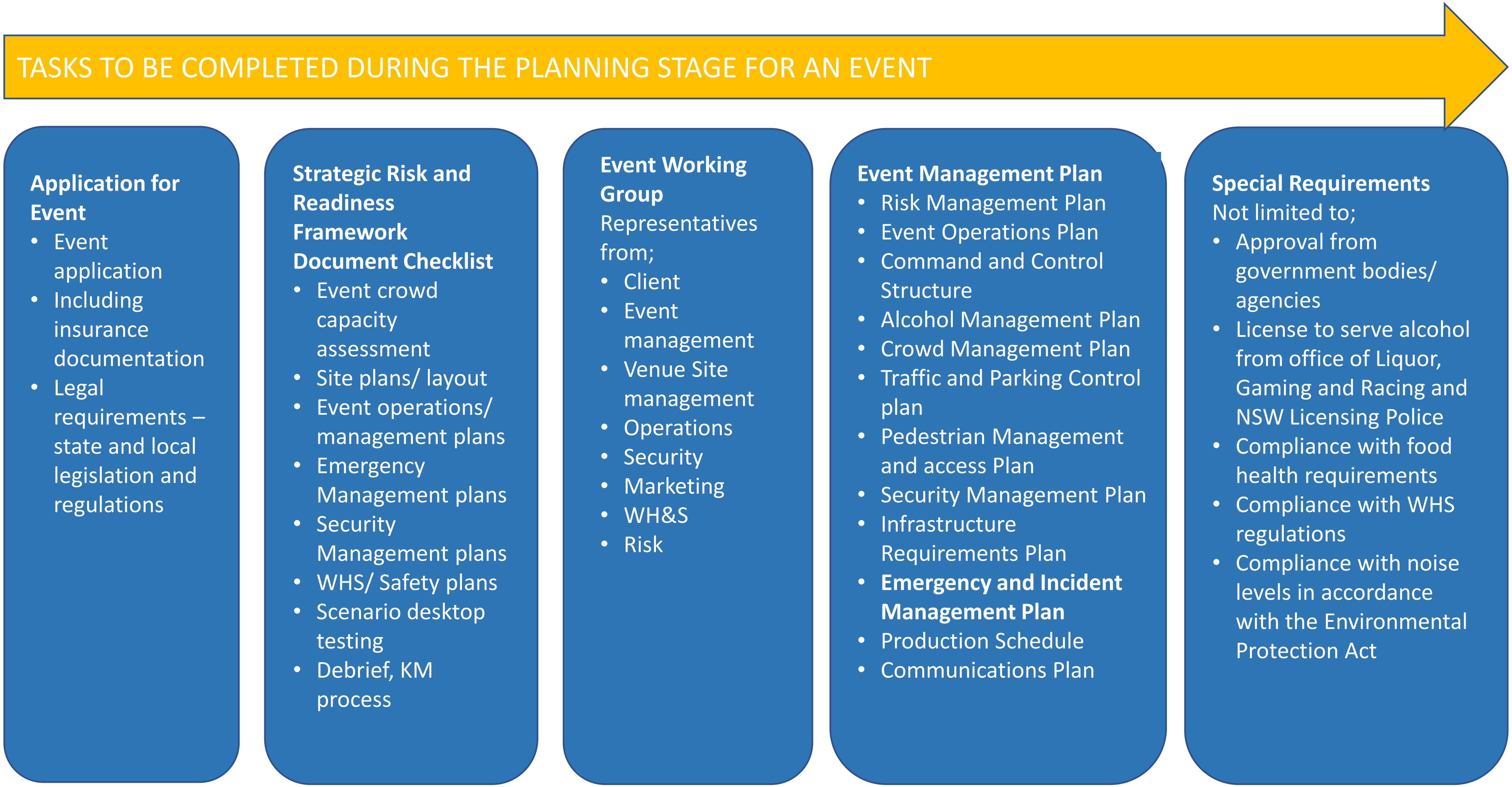
# Owner/ Operator Responsibilities

- The quality and quantity of planning vary depending on;
  - Nature of the event
  - Crowd expectations
  - Event management experience
- Inadequate planning will increase the risks associated with an event
- Risks need to be managed with appropriate planning and preparation
- Planning for public events requires strong cooperation between event organisers and government agencies
- Involving emergency management experts in the planning phases will contribute to a safer event

# How to Prepare

- Better understand the environment
- Monitor key issues and trends
- Review the organisations capabilities
- Review organisational procedures
- Review the measures and capability
- Implement continuous improvement

# Organisational Readiness Framework



TASKS TO BE COMPLETED DURING THE PLANNING STAGE FOR AN EVENT

**Application for Event**

- Event application
- Including insurance documentation
- Legal requirements – state and local legislation and regulations

**Strategic Risk and Readiness Framework Document Checklist**

- Event crowd capacity assessment
- Site plans/ layout
- Event operations/ management plans
- Emergency Management plans
- Security Management plans
- WHS/ Safety plans
- Scenario desktop testing
- Debrief, KM process

**Event Working Group**

Representatives from;

- Client
- Event management
- Venue Site management
- Operations
- Security
- Marketing
- WH&S
- Risk

**Event Management Plan**

- Risk Management Plan
- Event Operations Plan
- Command and Control Structure
- Alcohol Management Plan
- Crowd Management Plan
- Traffic and Parking Control plan
- Pedestrian Management and access Plan
- Security Management Plan
- Infrastructure Requirements Plan
- **Emergency and Incident Management Plan**
- Production Schedule
- Communications Plan

**Special Requirements**

Not limited to;

- Approval from government bodies/ agencies
- License to serve alcohol from office of Liquor, Gaming and Racing and NSW Licensing Police
- Compliance with food health requirements
- Compliance with WHS regulations
- Compliance with noise levels in accordance with the Environmental Protection Act

# Security Principles

- Adopt a security in depth approach
- Multi layer security infrastructure
- An “outside – in” defensive approach
- Consider security measures

# DDDRR Principle

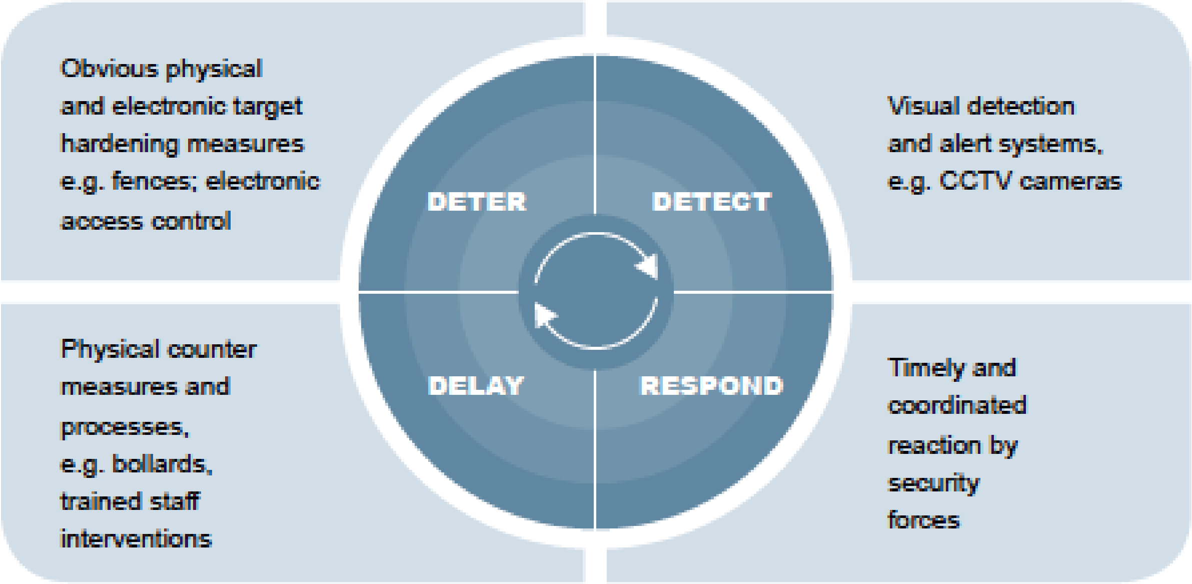
Deter Intruders

Detect Intruders

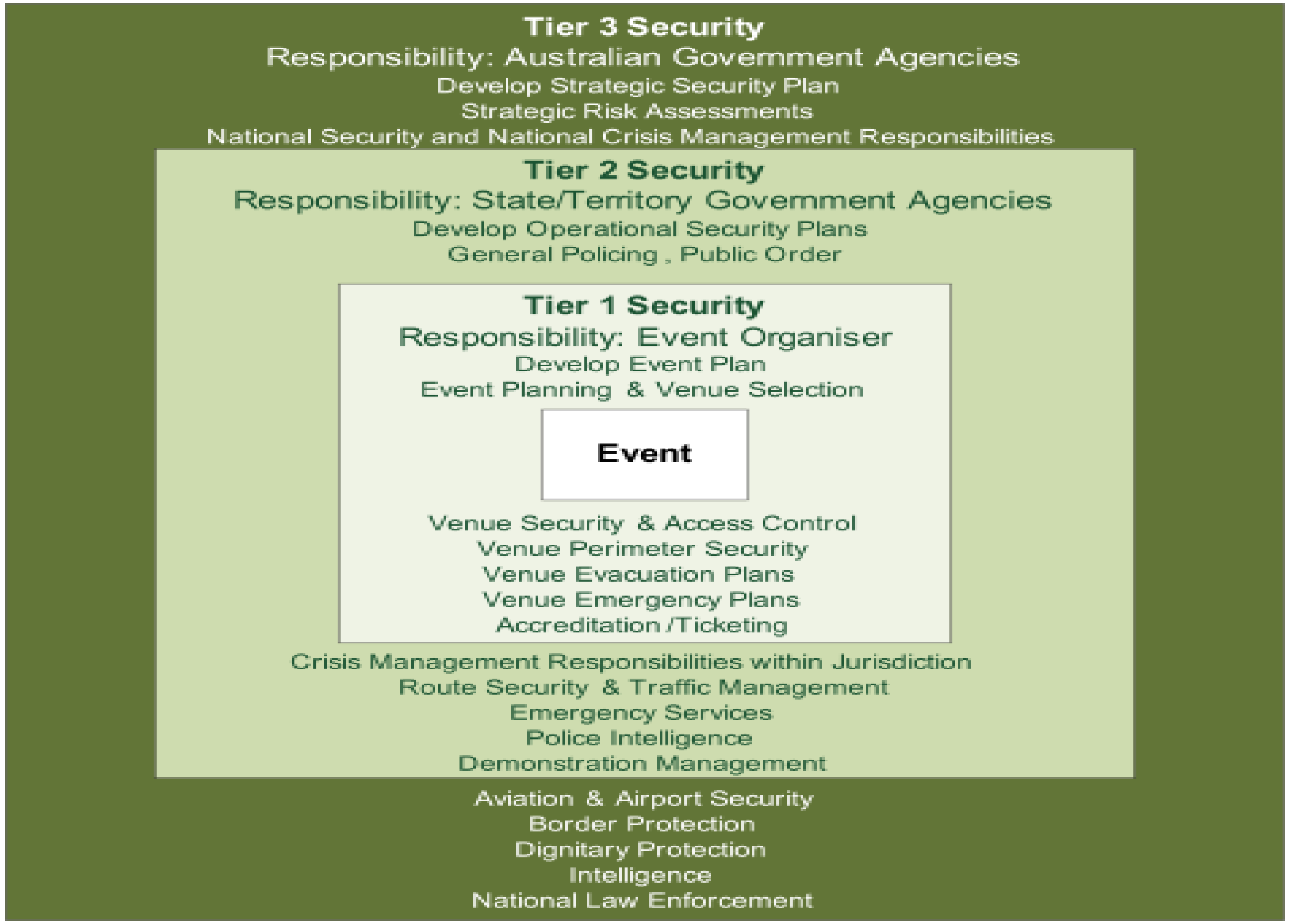
Delay Intruders

Respond to Intrusions

Recovery Plans


Obvious physical and electronic target hardening measures e.g. fences; electronic access control
DETER
DETECT
Visual detection and alert systems, e.g. CCTV cameras
Physical counter measures and processes, e.g. bollards, trained staff interventions
DELAY
RESPOND
Timely and coordinated reaction by security forces

# 3 Tier Security Model



**Tier 3 Security**

Responsibility: Australian Government Agencies

Develop Strategic Security Plan
Strategic Risk Assessments
National Security and National Crisis Management Responsibilities

**Tier 2 Security**

Responsibility: State/Territory Government Agencies

Develop Operational Security Plans
General Policing , Public Order

**Tier 1 Security**

Responsibility: Event Organiser

Develop Event Plan
Event Planning & Venue Selection

**Event**

Venue Security & Access Control
Venue Perimeter Security
Venue Evacuation Plans
Venue Emergency Plans
Accreditation /Ticketing

Crisis Management Responsibilities within Jurisdiction
Route Security & Traffic Management
Emergency Services
Police Intelligence
Demonstration Management

Aviation & Airport Security
Border Protection
Dignitary Protection
Intelligence
National Law Enforcement

# Considerations for Security Design

- Business continuity
- Security incident and evacuation
- Security escalation plans
- Emergency service response
- Security risks in the surrounding area;
- Vehicle and pedestrian traffic patterns
- The landscape in the surrounding area

# Risk Assessment

**RISK MANAGEMENT PLANNING**

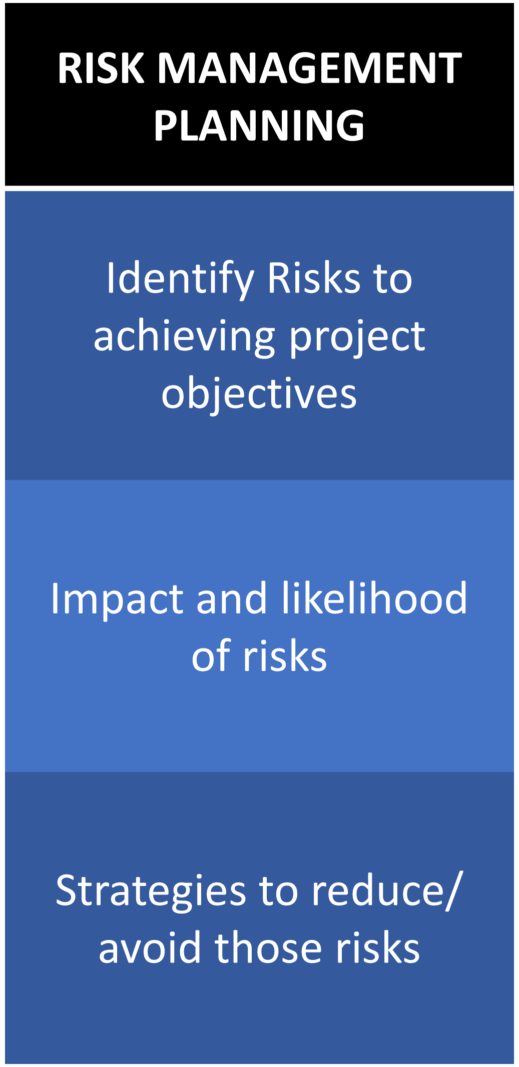
Identify Risks to achieving project objectives

Impact and likelihood of risks

Strategies to reduce/ avoid those risks

- Key to understanding your event from a safety and security perspective and what could potentially go wrong and result in an emergency incident response
- Provides evidence that you as an event manager have undertaken the necessary steps to identify the risks and ensure preparedness in the event of an incident associated with that risk
- Provides evidence that you have an understanding of responsible parties in the planning and response to an incident

# Risk Assessment



**RISK MANAGEMENT PLANNING**

Identify Risks to achieving project objectives

Impact and likelihood of risks

Strategies to reduce/ avoid those risks

- A key tool in communicating with other responsible parties what hazards and risks have been identified and treated to provide a level of safety and security to patrons attending the event.
- A key tool for making decisions around whether an identified risk or hazard is acceptable going into an event
- Completing a risk assessment provides evidence of an event organiser undertaking their obligation to provide a “duty of care” to all patrons attending the event

# Risk Assessment

- Engage State or Territory Police on current national and local security threats
- Obtain threat reports from Government Agencies
- Identify key business function and assets
- Identify the venue/ event vulnerabilities
- Identify and assess security risks
- Assess likelihood and consequence of security risks
- Implement protective security measures

# Key Risks Categories

- Public Safety / Worker Safety
- Terrorism - Active armed offender (weapons including knife, firearms, IED, hostile vehicle) – personal safety, potential mass injuries, crisis situation
- Crowd Management – personal safety, medical emergency, crowd crush
- Command, Control and Communication
- Security Management – access control, crowd behaviour
- Traffic Management
- Media Communications/ reputation
- Extreme Weather
- Infrastructure and Site Risks
- Production Risks
- Site Induction

# Risk Assessment

A risk assessment will assist in the development and redevelopment of important safety and security plans and requirements;

- Security Management plan
- Emergency Management plan
- Incident Management plan
- Crowd Management plan
- Traffic/ pedestrian  Management Plan
- Pre event tabletop exercises

# Risk Assessment

There is a suite of supplementary documents that can assist in the understanding and implementation of safety and security measures and response;

- Crowded places self assessment tool
- Crowded places security audit
- Hostile vehicle mitigation guidelines
- Active Armed offender guidelines
- Improvised Explosive Device Guidelines

# EAP Framework

Is the security management of the site;

**Effective:** must ensure that the measures are effective and possess some level of proven and successful capability in preventing an attack or mitigating an attack if it occurs.

**Appropriate:** must ensure that the measures reflect the level of threat and the likelihood of an attack.

**Proportionate**: must ensure that the measures reflect the level of vulnerability of a site or venue.

# Blast Treatments

- Maximise standoff distance from buildings and major areas of gathering
- Locate drop off zones away from places of mass gathering and main entrances
- Locate public parking as far away as possible from places of mass gathering
- Locate loading docks and delivery areas away from key areas and assets
- Implement Traffic exclusion zones
- Minimise areas for concealment

# Access Control

- Access points minimised
- Reception areas – hardened against unauthorised access
- Guard posts
- Security Screening
- Security Control Rooms
- Security Perimeter Fencing
- Safe rooms or areas – shelter in place

# Security Screening Checkpoints

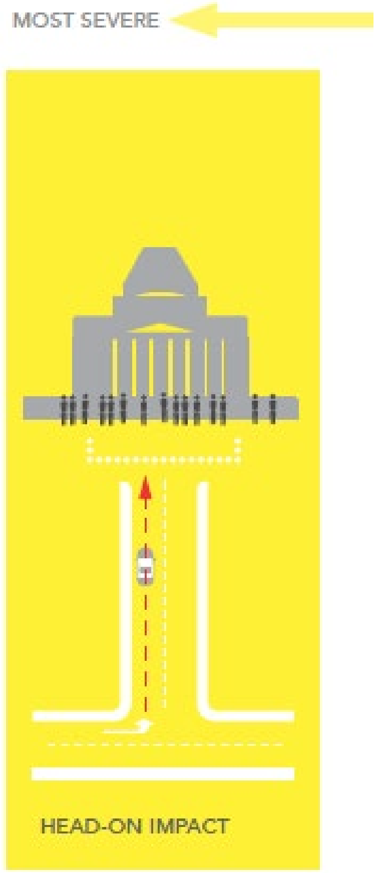
- Be clear on prohibited items
- Metal detectors (walk-through, hand-held and body scanner)
- X-ray equipment
- Explosive trace detection

# Security Screening Checkpoints

- allow sufficient and controlled space for visitor queuing;
- be designed so they cannot be bypassed;
- be designed to cater for immediate evacuation;
- be located as far away from key business functions and assets as possible;
- be located in an area that will minimise the physical impact of an attack;
- be supported by an access control system, CCTV coverage and security lighting;
- enable the secure storage of prohibited items;
- have clear line of sight of approaches to the entrance; and
- incorporate rejection paths for both individuals and small groups.

# Hostile Vehicle Vulnerability Assessment

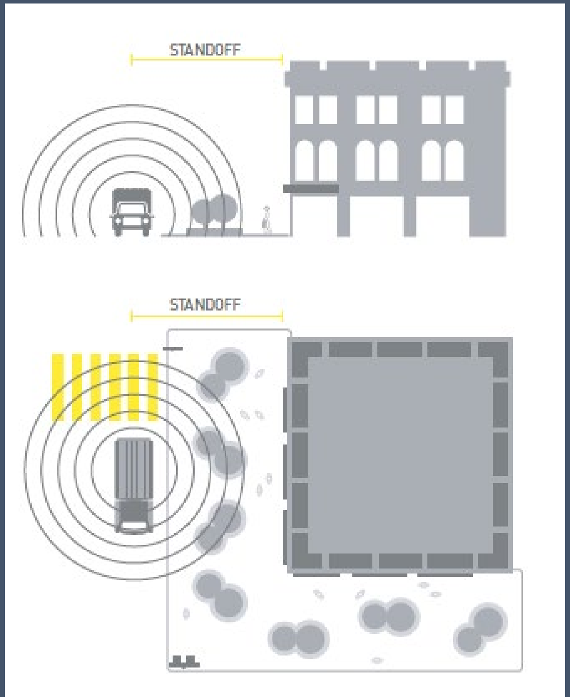
- Site inspection
- Identification of vulnerable locations
- Assessment conducted on each location
- Vehicle approach  - opportunity to increase velocity
- Impact angle - head on, in turn or angled
- Site rating High/ Medium/ Low
- Appropriate vehicle control measures recommended



# Hostile Vehicle Mitigation

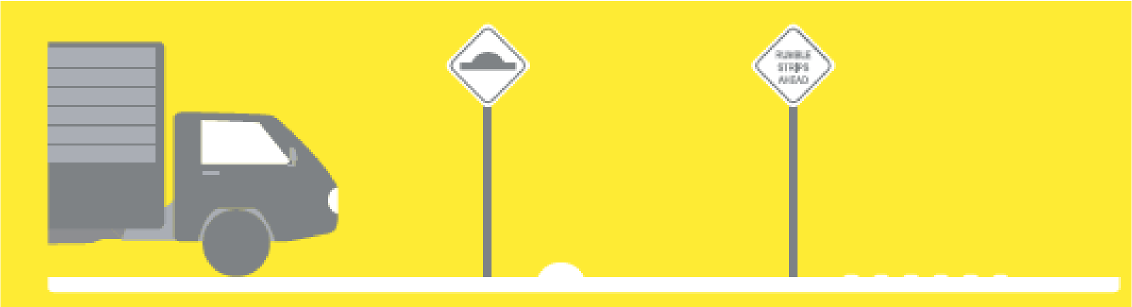
- High pedestrian traffic areas
- Congregation areas
- Venue assets
- Protection from unauthorised vehicle
- Traffic Management options
- Implementation of permanent PAS rated bollards/ barriers
- Elevated pathways, gardens
- Implementation of temporary rated barriers/ blocks

# Integrated Security Approach



## A Layered Approach

- Security is most effective when implemented with layers of HVM
- Access control and vehicle management
- The immediate vicinity of the asset (people, property, equipment) should be protected through further layers added at different standoff distances
- The security system must be equal to the assessed threat level whilst not impeding on the sites day to day operation
- Traffic Management options include;
  - Vehicle exclusion
  - Vehicle inclusion
  - Temporary protection (during heightened threat levels)
  - Traffic calming methods ( to slow vehicles)



# Crowd Management

- To help with crowd density and crowd movement;
- Separation of pedestrian and vehicle entry/access control points
- Manage the number of access points
- Consider the closing of route(s)
- redirection of pedestrians via alternative or more secure routes
- Efficient and effective search/screening of persons/vehicles to meet anticipated throughput

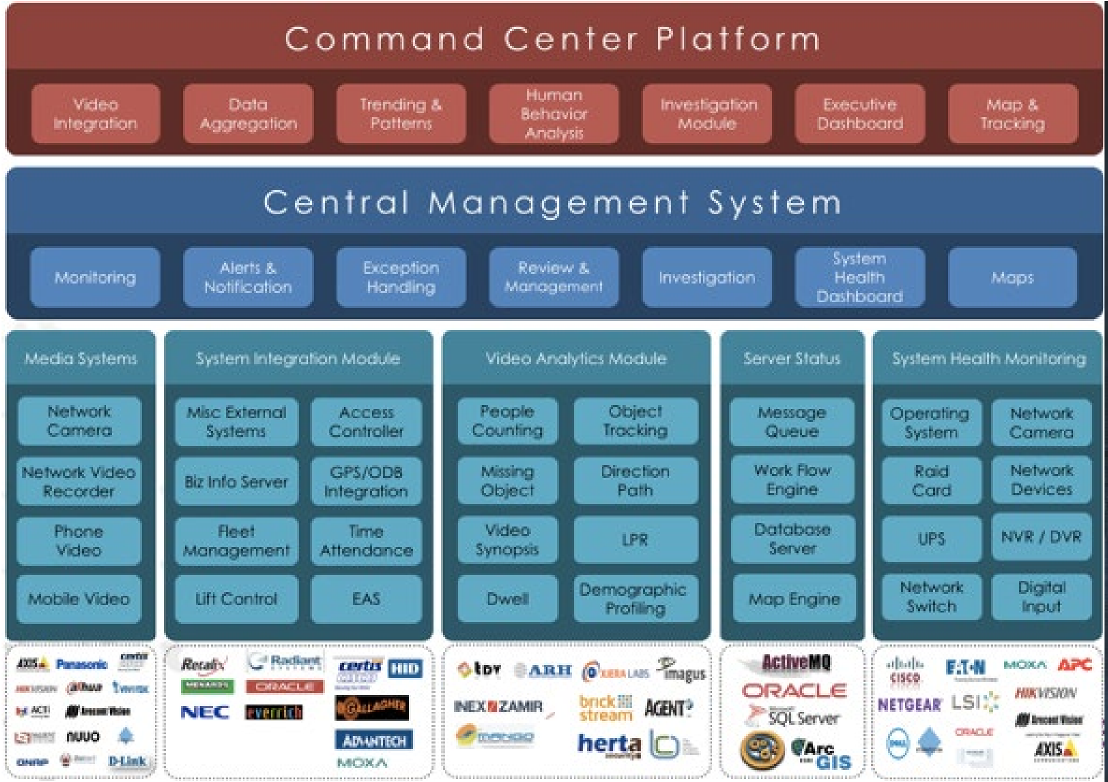
# Crowd Management

To help with crowd density and crowd movement;

- Procedures for pre-notification pass/ticket collection and person/pass/ticket verification.
- Orientation of access points, queues and approach routes to maximise spatial and situational awareness of the public.
- Stagger exit times, maximise exit routes and de-conflict peak periods with neighbouring events/sites.

# Technology

## FULLY INTEGRATED SECURITY PLATFORM



Command Center Platform

- Video Integration
- Data Aggregation
- Trending & Patterns
- Human Behavior Analysis
- Investigation Module
- Executive Dashboard
- Map & Tracking

Central Management System

- Monitoring
- Alerts & Notification
- Exception Handling
- Review & Management
- Investigation
- System Health Dashboard
- Maps

Media Systems

- Network Camera
- Network Video Recorder
- Phone Video
- Mobile Video

System Integration Module

- Misc External Systems
- Access Controller
- Biz Info Server
- GPS/ODB Integration
- Fleet Management
- Time Attendance
- Lift Control
- EAS

Video Analytics Module

- People Counting
- Object Tracking
- Missing Object
- Direction Path
- Video Synopsis
- LPR
- Dwell
- Demographic Profiling

Server Status

- Message Queue
- Work Flow Engine
- Database Server
- Map Engine

System Health Monitoring

- Operating System
- Network Camera
- Raid Card
- Network Devices
- UPS
- NVR / DVR
- Network Switch
- Digital Input

- Aggregated CCTV from all Systems, including mobile phones
- Next Generation Facial Recognition engine across all CCTV Cameras
- Facial Recognition on all Security Officers – locally scanning on device

SCG
sheridan consulting group

# Emergency Management

- Event / venue Emergency Management plan
- Emergency Control Organisation – Chief Warden etc
- Emergency Vehicle Access
- Emergency Evacuation - gates, routes and assembly areas
- Emergency communication systems
- Emergency communication systems are typically operated from a secure area—for example, security control room or event operations centre.
  one-way systems enable communications to be broadcast to many people;
- two-way systems enable communication between Emergency Control Organisation, Wardens as well as emergency response personnel.

# Exercises and Drills to test planning, response and recovery

**Crisis Management Tabletop Exercise**

Crisis Management tabletop exercises conducted as part of the Business Continuity Management Plan should involve or be conducted in relation to a major security incident/terrorist attack.

**Major Security Incident Simulation**

A major security incident simulation should be conducted, and will involve physically acting out the incident response, crisis management and/or business continuity action plans in a controlled environment in relation to a terrorist attack scenario.

# Safety and Security Operations Plan

- Ensure security is a permanent feature
- Personal commitment by senior management
- Staff guidelines are clear
- Internal communications to promote security awareness
- Effective screening processes
- Staff security training
- Security exercises
- Self initiation security penetration and breach testing
- Reward and recognition program for staff

# Business Continuity Planning

- Regularly review risk assessments and business continuity plans
- Include escalation plans for response to heightened threat environment or direct threat
- Regularly review and test security procedures, emergency
- Maintain relationships with emergency services
- Consider increasing monitoring and detection capabilities
- Ensure any access restrictions are enforced
- Test security infrastructure to ensure it is operational

# Security Awareness

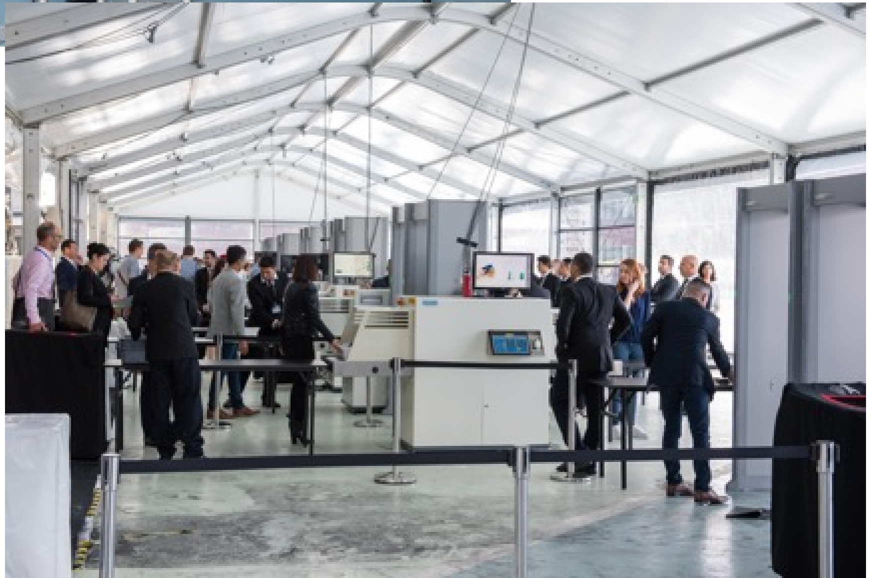
Security awareness training should cover:

- Current threat context and background on terrorism;
- How to conduct risk assessments using proven methods
- Recognising suspicious behaviour that may constitute pre-attack stages of terrorism;
- Emergency response procedures and strategies for responding to  a terrorist attack;
- How to manage and recover from a terrorist attack, integrated with the current Business Continuity Plan and procedures.

# Case Study: Major Events Sydney CBD Hostile Vehicle Mitigation

- Conduct vulnerability assessments
  - Approach to the site
  - Ability for a vehicle to pick up speed
  - Impact rating H/M/L
- Suitability of a layered perimeter approach
- Road closures and TCPs enforced by Police
- Additional controls implemented close to vulnerable sites including water filled barriers and heavy emergency vehicles – fire trucks and police vehicles

# Case Study: Salesforce World Tour Event Security



Increased security levels based on Event type and threat environment;

- Complete Risk and Vulnerability Assessment
- Patron security screening  - mag and bag
- Pre event registration – ticketed & ID’s displayed
- 24 hour security guarding
- Canine Explosive Substance Detection sweep
- Venue CCTV
- White level inspections
- Security logs for each day
- Shift handover completed by Security Manager
- Procedures response actions
- Site maps with security positions displayed
- Command, communications and control structure
- Green zone lockdown

# Case Study: Vivid Sydney
# VSRMF – Strategic and Operational Risk Assessments

The Vivid Sydney Risk Management Framework (VSRMF) which addresses three levels of risk;

**Level 1 Strategic Risks**: those that apply to Destination NSW as a whole and could adversely affect the achievement of the Organisations objectives and are managed by the DNSW Executive

**Level 2 Operational Risks**: those that may impact delivery of the Event and are managed by the Vivid Sydney Operational Team

**Level 3 Project Risks**: those risks that relate to the delivery of key functional programs or areas that are managed by contractors with responsibility for those those functional programs or areas

# Case Study: Vivid Sydney
# VSRMF – Strategic and Operational Risk Assessments

The Vivid Sydney Risk Management Framework

- Applies across all components of the event
- Foundational component which drives and influences the planning, documentation and management process
- The VSRMF has been developed through ongoing stakeholder consultation and will continue to do so based on the nature of the event

The framework includes;

- Vivid Sydney Benchmark Operational Risk Register
- Project Risk Map

# Case Study: Vivid Sydney
# VSRMF – Strategic and Operational Risk Assessments

The Vivid Sydney Benchmark Operational Risk Register has been developed to provide guidance and drive consistency in;

- Assessing risks types across the different event precincts
- Applying appropriate risk mitigation strategies
- Assessing and applying the residual risk rating
- Identifying the Responsible person/s correctly

# Case Study: NYE Sydney Integrated Crowd Management Plan

- The ICMP provides a strategy across multiple landholder and agency operational plans to facilitate the management of crowds for NYE 2017 in Sydney CBD

- Required identification and commitment of a stakeholder working committee

- The NSW Whole of Government Crowd Management Guidelines were issued by DPC to formalise and enhance the process of crowd safety for mass events

- The plan has evolved over the past couple of years – through learnings

# Case Study: NYE Sydney
# Integrated Crowd Management Plan

- The ICMP takes into account the changing landscape impacts eg. Light Rail construction
- The ICMP takes into account risk assessments and high rated vulnerable locations
- The ICMP requires consistent principles and strategies across all planning documents that manage movement of crowds
- Wayfinding plans
- Communications Plans
- Collaborative process with early planning cycle for effective integration of planning
- Major interaction between the ICMP and key planning documents

# Common Measures for Consistency of Safety Practices

- Maintain an awareness of the National Threat Advisory System
- Information sharing with Government, Police, similar venues/ events and neighbouring properties
- Implementation of standardised documentation and legislation in Emergency Security, Crowd and Risk Management
- Consistency in Command, Control, Coordination and Communication
- Clear and concise communication from a central area of control
- Security and safety planning, regular review and continuous improvement to be routine in the workplace