Infrastructure NSW

Walsh Bay Arts Precinct

Security Risk Management Report

251710-SE-SRA-01

Rev 02 | 4 November 2016

Job number 251710

Arup
Arup Pty Ltd ABN 18 000 966 165

Arup
Level 10 201 Kent Street
PO Box 76 Millers Point
Sydney 2000
Australia
www.arup.com

ARUP

Document Verification

ARUP

Job title		Walsh Bay Arts Precinct			**Job number** 251710
Document title		Security Risk Management Report			**File reference**
Document ref		251710-SE-SRA-01			
Revision	**Date**	**Filename**	SRA Report Template 01.docx		
Rev 01	10 Oct 2016	**Description**	Draft for client comment		
			Prepared by	Checked by	Approved by
		Name	Chris Nunn	Shane Norton	Elaine Clarke
		Signature			
Rev 02	4 Nov 2016	**Filename**			
		Description	SSDA		
			Prepared by	Checked by	Approved by
		Name	Chris Nunn	Shane Norton	Elaine Clarke
		Signature			
		Filename			
		Description			
			Prepared by	Checked by	Approved by
		Name			
		Signature			
		Filename			
		Description			
			Prepared by	Checked by	Approved by
		Name			
		Signature			
				Issue Document Verification with Document	✓

Contents

1 Executive Summary

Overview

Arup have been engaged by Infrastructure NSW (INSW) to assist them to manage their security risks at the Walsh Bay Arts Precinct, in Sydney.

This security risk management report identifies security risks relevant to the Walsh Bay Arts Precinct (WBAP) Project, provides an analysis and evaluation of those risks, and recommends treatment measures in order to reduce those risks to as low as reasonably practicable.

Method of Analysis

The security risk assessment (SRA) methodology used in this report has been based on the International Standard ISO 31000:2009 – Risk Management – Principles and Guidelines, and HB 167:2006 Security Risk Management.

Findings

This report has found that the security risk profile for the WBAP Project is generally tolerable or acceptable. The SRA process has examined the WBAP and identified 72 security related risks (refer to Section 7.4).

Of the 72 identified security risks, 0 were assessed as Extreme (Unacceptable risks), 15 were assessed as High (May be Tolerable), 31 were assessed as Medium (Tolerable), and 26 were assessed as Low (Broadly Acceptable).

All of the identified High and Medium security risks are either high consequence but low likelihood, or high likelihood but low consequence events. These risks are therefore more tolerable.

This report has also found that the crime rate for the City of Sydney Local Government Area (LGA), within which the WBAP is located, is quite high, however the offence rates are distorted due to the high number of people who frequent the area each day, and the relatively low population. The crime rate within the Sydney LGA is also declining, with 7 of the 10 most prevalent offences applicable to the WBAP reducing in occurrence over the previous 3 and 5 years. Based on these trends, the likelihood of these offences occurring in the future should generally either remain the same as currently assessed, or reduce.

Based on the outcome of this security risk assessment, all identified security risks can be tolerated if it is not reasonably practicable to reduce the risk further. However, if there are options for further risk reduction and the cost is proportionate to the benefits to be gained, then implementation of these measures should be considered.

Recommendations

A broad range of security treatment measures have been recommended in Section 11 to help mitigate and treat the identified security risks that the WBAP is exposed to, and lower them as low as reasonably practicable. The recommended

security treatment measures are based on Australian Security Standards, current security theories and reasonable security and security risk management practices. Recommended security treatment measures include the use of electronic and physical security measures, security management measures, and crime prevention through environmental design (CPTED) principles.

The assessed High risks should be prioritised, however as the High risks are all terrorist based risks that have been assessed as Rare or Unlikely, reasonable measures should only be implemented where practical.

Report Limitations

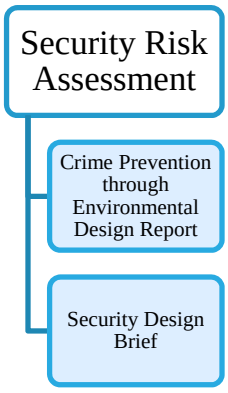
This security risk assessment has been based on the publically available Bureau of Crime Statistics and Research (BOCSAR) and Australian Bureau of Statistics Census data. As risks can change rapidly it is recommended that the risk profile of the WBAP is reviewed regularly in line with Section 12.3 and action taken accordingly.

Any opinion on terrorist type risks is based on Arup's limited ability to gather accurate and timely intelligence on the motivation, capabilities and resources of these threat sources. This is in particular, only through open source (publically available) gathering techniques.

Security reports document list

This document forms part of a developing family of security reports that Arup are producing as part of our professional services to the Walsh Bay Arts Precinct Project. The Security Risk Assessment is the overarching security document supported by more detailed advice provided in Crime Prevention through Environmental Design Report and Security Design Brief.

The Security Risk Assessment provides a broad identification of the threat and risk profile facing the WBAP, and outlines possible treatments. These treatments are then detailed in the underlying reports.



Conclusions

This report has been based on international standard practices. This report has found that all of the 72 identified security risks may be tolerable or are broadly acceptable.

Based on the outcome of this security risk assessment, all identified security risks can be tolerated if it is not reasonably practicable to reduce the risk further, however reasonable treatment measures have been recommended in order to reduce the identified risks to as low as reasonably practicable.

2 Introduction

2.1 Document Purpose

The purpose of this security risk assessment is to identify, analyse, and evaluate potential security risks that the WBAP is exposed to, and to recommend reasonable measures to reduce the risks' likelihood and/or consequence to as low as reasonably practicable.

2.2 Project Context

The vision for the WBAP is to create a landmark waterfront destination that supports world-class productions and delivers memorable experiences for people from Sydney, across NSW and international visitors. The redevelopment will boost Sydney's reputation as an innovative, culturally competitive city within the Asia Pacific region.

The Walsh Bay Arts Precinct encompasses Pier 2/3, and Wharf 4/5, all located within a unique waterfront and heritage setting.

The redevelopment includes creating new arts facilities and performance venues in Pier 2/3, refurbishing facilities in Wharf 4/5 and providing a new waterfront square between them for outdoor performances, festivals, public art, commercial and community activities. It will more than double the arts offerings at Walsh Bay with new and upgraded production, rehearsal, studio and performance venues.

2.3 Methodology

The security risk assessment methodology used to produce this report has been based on the International Standard ISO 31000:2009 – Risk Management – Principles and Guidelines, and the HB 167 – 2006: Security Risk Management Handbook.

The methodology encompassed the following process:

- Communicate and consult with key stakeholders throughout the security risk assessment process;
- Perform a review of existing project documentation in order to help establish the context of the SRA including internal and external environmental factors;
- Undertake a site inspection in order to better understand its layout, operations, challenges, constraints, vulnerability, and to identify its critical assets;
- Research, review, and analyse relevant national, state, LGA, suburb, and locality data in order to gain an understanding of external environmental factors that may affect the WBAP;

- Identify sources of risk that the WBAP is exposed to, and identify any existing security treatment measures;
- Analyse the identified security risks, and relevant crime trends of these identified security risks;
- Evaluate the identified security risks to determine the tolerance of these risks, evaluate the need to treat these risks, and to determine which risks to prioritise treatment of;
- Provide recommendations for security mitigation treatments for the identified security risks;
- Produce a preliminary Security Risk Assessment Report as part of the State Significant Development Application (SSDA) ;
- Following the approval of the SSDA designs, hold a security workshop with the key stakeholders to discuss key security and CPTED considerations based on the SSDA design documentation; and
- Produce a final Security Risk Assessment Report as part of the Phase 3 Design Documentation incorporating the outcomes of the stakeholder workshop.

3 Acronyms and Definitions

3.1 Acronyms

Table 1 – Acronyms

Acronym	Description
ALARP	As Low As Reasonably Practicable
ASIO	Australian Security Intelligence Organisation
BOCSAR	NSW Bureau of Crime Statistics and Research
CBD	Central Business District
CBR	Chemical/ Biological/ Radiological
CCTV	Closed Circuit Television
EAC	Electronic Access Control
EACS	Electronic Access Control System
GTD	Global Terrorism Database
IAS	Intruder Alarm System
INSW	Infrastructure NSW
HVM	Hostile Vehicle Mitigation
IED	Improvised Explosive Device
ISO	International Standard Organisation
LGA	Local Government Area
NSW	New South Wales
NSWPF	New South Wales Police Force
SCEC	Security Construction and Equipment Committee

Acronym	Description
START	National Consortium for the Study of Terrorism and Responses to Terrorism
SRA	Security Risk Assessment
SSDA	State Significant Development Application

3.2 Definitions

Table 2 - Definitions

Term	Definition
Assault: Non-domestic violence related	Direct (and immediate/confrontational) infliction of force, injury or violence upon a person or persons or the direct (and immediate/confrontational) threat of force, injury or violence where there is an apprehension that the threat could be enacted. Includes the police incident categories of actual bodily harm, common assault, grievous bodily harm (including malicious wounding), shoot with intent other than to murder, assault police officer and spike drink/food. Not deemed to be domestic violence related.
Asset	An item or process that an individual, community or Government values and is important to supporting the expectations of those people's, organisations' or Government's outcomes and objectives.
Break and enter – Non dwelling	Unlawful entry of a structure with the intent to commit an offence where the entry is either forced or unforced. Break and enter can occur in dwellings or non-dwellings. Non-dwellings include premises where people do not usually reside such as retail premises, wholesale premises, educational premises, industrial premises, recreational premises etc.
Business continuity management	Business Continuity Management provides for the availability of processes and resources in order to ensure the continued achievement of critical objectives.
Capability	The ability, experience and knowledge of a person, process or information to undertake the stated or claimed activity. This is commonly used in relation to the capability of a threat source.
Consequence	The outcome of an event affecting objectives.
Context	A summary of the key internal and external issues that could influence the risks under examination or decisions about those risks.
Control	Any existing physical, behavioural, institutional, or cultural mechanism by which a risk is managed.

Term	Definition
Criticality	The importance or dependence that an organisation has on a person, function, process, item or infrastructure or specific facility.
Event	Occurrence of a particular set of circumstances.
Harassment, threatening behaviour and private nuisance	Actions that harass or are intended to harass, threaten or invade the privacy of an individual, not amounting to an assault, sexual assault, blackmail or intimidation. Can be face to face, written, or made through a carriage service (e.g. phone, computer, etc.). Includes the police incident categories of intimidation (includes stalking), telecommunications offences, threats against police, riot and affray, unlawful assembly, and violent disorder.
Impact	The outcome following the occurrence of an event.
Intent	The confidence to carry out the stated or postured claim and the desire to carry out the action or activities.
Likelihood	The chance of something happening.
Malicious damage to property	Wilful and unlawful destruction, damage or defacement of public or private property or the pollution of property or a definable entity held in common by the community. Includes the police incident categories of graffiti, malicious damage to property, public place - damage fountain/wall etc. and public place - damage shrine/monument.
Offensive conduct	Nonverbal behaviour that is likely to be considered offensive by another person. Includes the police incident category of offensive conduct.
Organisation	A company, firm, organisation, association, group or other legal entity or part thereof, whether incorporated or not, public or private, that has its own function(s) and administration.
Other theft	Includes the police incident categories of steal from marine vessels, steal vessels, other stealing occurring somewhere other than a residential dwelling (e.g. at temporary accommodation, business/commercial premises, in outdoor/public places).
Resilience	The ability or capacity to recover from harm.
Risk	A combination of the consequences of an event and the associated likelihood of occurrence.
Root causes	Underlying conditions that may give rise to threats, hazards and other sources of risk. Within a security context this may include factors such as social and economic conditions (poverty, injustice, political aspirations, alienation, etc.).
Security	The preparedness, protection and preservation of people, property and information, both tangible and intangible.
Security incident	A ‘security incident’ is regarded as any event or circumstance involving or affecting the individual, community or organisation that causes or is likely to

Term	Definition
	cause a loss (physical or otherwise), disruption, or fear arising from the deliberate activities of other parties. Whose impacts are, or could potentially be realised against people, property or information.
Security risk assessment	The identification, analysis, and evaluation of security risks.
Security risk management	The culture, processes, and structures that are directed towards the effective management of potential adverse consequences against people, property, or information.
Security risk management process	A process built on effective communication and consultation with stakeholders, comprising the identification of security risks, their analysis and evaluation within the relevant context, their reasonable treatment, continuous monitoring, and regular review.
Stakeholders	Those people and organisations who may affect, be affected by, or perceive themselves to be affected by, a decision, activity, or event.
Steal from motor vehicle	Unlawful taking of parts or contents from another person's motor vehicle illegally and without permission. Includes the police incident category of 'steal from motor vehicle'.
Steal from person	Taking money or personal goods, whether from the immediate possession or control of a person without the use of force, threat of force or violence or putting the victim in fear. Includes the police incident category of 'steal from person'.
Threat	Anything that has the potential to prevent or hinder the achievement of objectives or disrupt the processes that support them. A source of, or potential for harm to occur. A threat can be a source of risk.
Threat source	A list of potential sources that could cause harm to an organisation. For example, a vandal, a disgruntled former employee, a criminal, stakeholders, customers, or a terrorist.
Treatment measure	A control applicable to identified risks.
Vulnerability	Any weakness that can be exploited by an aggressor to make an asset susceptible to change.

4 Security Risk Management

4.1 Overview

Security risk management refers to the culture, processes, and structures that are directed towards the effective management of potential adverse consequences that may affect people, property, or information.

The security risk management process detailed in Section 4.3 below, is built on effective communication and consultation with stakeholders, and comprises the identification of security risks, their analysis and evaluation within the relevant context, their reasonable treatment, their continuous monitoring, and their regular review.

The sections below define risk, likelihood, and consequence within this security risk management context. The sections below also outline the security risk management process followed, and the security risk matrix used as part of this security risk assessment.

4.2 Definition of Risk

Many definitions of risk exist, and many different risk definitions and formulas are used for risk management and security risk management purposes. Each risk definition and formula have their respective pros and cons.

For this security risk assessment, the standard risk management definition, as defined in ISO 31000 – Risk Management, has been used.

Risk has been defined as:

Risk = Consequence x Likelihood

Where:

- **Risk** is a combination of the consequences of an event and the associated likelihood of occurrence;
- **Consequence** is the outcome of an event affecting objectives; and
- **Likelihood** is the chance of something happening.

In risk management, consequences can be either positive or negative, whereas in security risk management, consequences can only be negative.

4.3 Security Risk Management Process

The security risk management process followed for this security risk management report has been based on the ISO 31000 risk management process, outlined in the figure below:

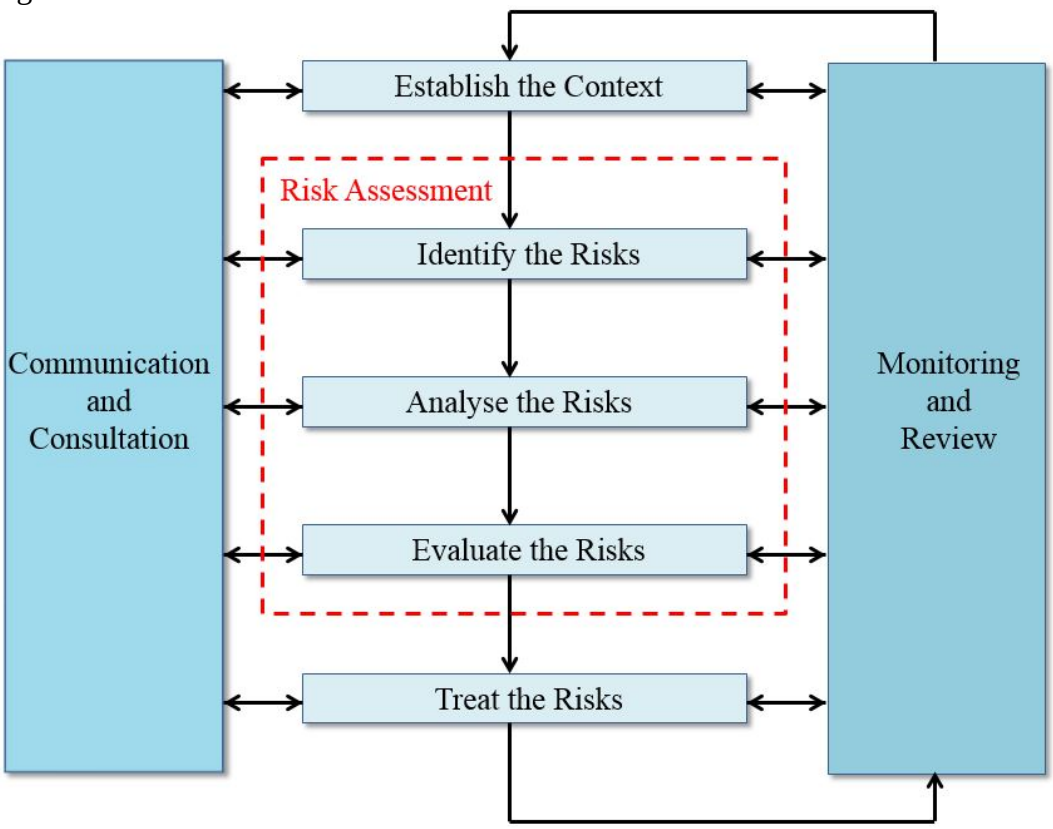


Figure 1 – Security Risk Management Process

4.4 Risk Assessment Matrices

The security risk rating matrix, and security risk tolerance, likelihood, and consequence definitions detailed below have been used as part of this security risk assessment process, and have been derived from HB 167 Security Risk Management.

4.4.1 Security Risk Rating Matrix

Table 3 - Security Risk Matrix

	Consequence				
Likelihood	Minimal	Minor	Moderate	Major	Catastrophic
Almost Certain	Medium	Medium	High	Extreme	Extreme
Likely	Medium	Medium	Medium	High	Extreme
Possible	Low	Medium	Medium	High	High
Unlikely	Low	Low	Medium	Medium	High
Rare	Low	Low	Medium	Medium	High

4.4.2 Security Risk Tolerance Definitions

Table 4 - Security Risk Tolerance Definitions

Classification		Risk Tolerance
Extreme	Unacceptable	Extreme risks are regarded as unacceptable where the risk cannot be justified, except in extraordinary circumstances.
High	May be Tolerable	High risks may be tolerable only if further risk reduction is impracticable (for example because of cost benefit considerations or an absence of a feasible solution).
Medium	Tolerable	Medium risks are regarded as tolerable only if further risk reduction is impracticable (for example because of cost benefit considerations or an absence of a feasible solution).
Low	Broadly Acceptable	Risks with this ranking are considered to be broadly acceptable, where risk reduction is not likely to be required as any benefits realised are likely to be outweighed by costs. These risks will be treated where reasonable and practical.

4.4.3 Security Risk Likelihood Definitions

Table 5 - Security Risk Likelihood Definitions

Likelihood	Criteria
Almost certain	• Over 99% probability, or • 'happens often', or • could occur within 'days to weeks'
Likely	• >50% probability, or • 'could easily happen', or • could occur within 'weeks to months'
Possible	• >10% probability, or • 'could happen, has occurred before', or • could occur within 'a year or so'
Unlikely	• >1% probability, or • 'has not happened yet, but could', or • could occur 'after several years'
Rare	• <1% probability • 'conceivable but only in extreme circumstances' • exceptionally unlikely, even in the long term future • a '100 year event' or greater

4.4.4 Security Risk Consequence Definitions

Table 6 - Security Risk Consequence Definitions

Consequence Rating	Financial Consequence	Reputational Consequence	Project/Business Consequence
Catastrophic	Corporate: > $100,000,000 Local: (> $5,000,000)	Extreme negative coverage causing public outcry appearing consistently over weeks Majority of stakeholders severely disadvantaged (months)	Serious process breakdown that prevents the achievement of mission critical objectives Multiple severe injuries, including fatalities
Major	Corporate: $5,000,000 - $100,000,000 Local: (< $5,000,000)	Negative significant coverage, appearing consistently over weeks Multiple stakeholders severely disadvantaged (weeks - months)	Serious process breakdown that substantially impedes the achievement of a core objective Multiple severe injuries, or a single fatality
Moderate	Corporate: $50,000 - $5,000,000 Local: (< $50,000)	Negative coverage lasting for several days, and/or frequent reoccurrence for several weeks Multiple stakeholders experience significant disadvantage (weeks)	Process breakdown that impedes the achievement of an important objective or causes extensive inefficiencies in key processes Multiple casualties requiring hospital attention
Minor	Corporate: $2,000 – $50,000 Local: (< $10,000)	Minor negative coverage, limited circulation for one day Minority of stakeholders experience disadvantage (days - weeks)	Process breakdown that impedes the achievement of one or more objectives or some inefficiencies in key processes Minor injuries requiring medical attention
Minimal	Corporate: < $2000 Local: (< $1000)	Isolated brief coverage, single media outlet Stakeholders experience minimal disadvantage (days)	Process breakdown or inefficiencies that have a limited impact on the achievement of an objective Minor injury requiring first aid only

5 Communication and Consultation

5.1 Overview

Communication and consultation are a necessary part of each step of the security risk management process. Stakeholders should be consulted as part of this process, and the sections below document how this was achieved.

5.2 Benefits of Consultation

The value of taking a consultative team approach throughout the security risk management process may:

- Help establish the context appropriately;
- Ensure that the interests of stakeholders are understood and considered;
- Help ensure that risks are adequately identified;
- Bring different areas of expertise together for analysing risks;
- Ensure that different views are appropriately considered when defining risk criteria and in evaluating risks;
- Secure endorsement and support for a treatment plan;
- Enhance appropriate change management during the risk management process; and
- Develop an appropriate external and internal communication and consultation plan.

5.3 Stakeholder Consultation

Continual Consultation

Consultation with key project stakeholders has and will continue throughout the project program. Key stakeholders consulted as part of the security works includes, but was not limited to:

- INSW;
- Arts NSW;
- MG Planning;
- MI Associates;
- TZG Architects; and
- McGregor Coxall.

Stakeholder Workshop

A stakeholder workshop will be held during Phase 3 Design Development, and will be based on the approved SSDA designs. Stakeholder input will be sought in order to gain a greater understanding of the site itself, how it operates, and any design risks. Stakeholder input will also be sought into but not limited to the following:

- Any security risks not covered by this SRA;
- Any identified security risks that are not relevant;
- The assessed risk ratings;
- Critical assets;
- Critical functions;
- Organisational vulnerabilities;
- Treatment measures; and
- Key aspects of the design from a security, security risk management, and CPTED perspective.

6 Context Establishment

6.1 Overview

Security risk management needs to be conducted in a manner that is appropriate to the organisation's type, culture, operational issues and the wider environment within which it operates. In particular, security risk management needs to be appropriate to the prevailing and emerging security risk environment.

Establishing the context is critical because it sets the basis on which all subsequent security risk management activities are conducted. The external context within which the WBAP operates, and the internal context of WBAP are examined below.

6.2 External Context

6.2.1 Overview

The term 'external context' refers to gaining an understanding of the external environment in which the WBAP is operating or may be operating in the future. In assessing the external context, the key objective is to identify and characterise factors in the external environment that are going to have an effect on the WBAP. Ultimately, the focus will be on those factors which will either directly or indirectly have security risk implications for the WBAP.

This section therefore establishes the community, socio-economic, market, and geopolitical context within which the WBAP operates.

6.2.2 Community Context

Overview

The community context profiles the site and suburb within which the WBAP is located, profiles the local population, and examines the local infrastructure and social infrastructure of the area.

Site Location

The WBAP is located in Walsh Bay, off Hickson Road, Sydney. The WBAP is located between Dawes Point and Millers Point.

Suburb Profile

The suburb of Sydney largely comprises the Sydney central business district. The central business district of Sydney is roughly bounded by Circular Quay and Sydney Harbour to the north, Macquarie Street to the east, Darling Harbour to the west and Liverpool Street and Central railway station to the south.

Based on information collected during the 2011 Census (most current available information), Sydney is largely an overseas born suburb with 82.8% of residents

being born overseas compared to the NSW average of 31.4%. Sydney has a relatively high Chinese, Indonesian, Thai and Korean population.

Sydney has above average income levels and has 47.7% of residents employed as either Professionals or Managers, which is higher than the state average of 36%. Sydney has below average representation in the technician, trade workers, labourers, and machinery operators and drivers professions.

Sydney has a significantly higher representation within the Cafes, Restaurants, & Takeaway Food Services, the Legal and Accounting Services, the Depository Financial Intermediation, the Computer System Design and Related Services, and the Auxiliary Finance and Investment Services industries.

Sydney is a high density residential suburb with 97.3% of dwellings either units, flats or apartments, compared to the state average of 18.8%. 63.4% of residents within Sydney are renters, compared to the state average of 30.1%.

Table 7 - Population and Infrastructure Profile

Indicator	Percentage	NSW Average
Population	14,308 (Total)	N/A
Males	51.4%	49.3%
Females	48.6%	50.7%
Australian Born	17.2%	68.6%
Overseas Born	82.8%	31.4%
Indigenous	0.1%	1.0%
Age Structure		
Aged 0-14 years	4.1%	19.2%
15-29 years	48.1%	19.7%
30-44 years	28.9%	20.9%
45-64 years	14.1%	25.5%
Aged 65+	4.8%	14.7%
Median Age	29	38
Birth Place		
Australia	17.2%	68.6%
China	11.7%	2.3%
Indonesia	9.3%	0.4%
Thailand	7.1%	0.3%
Korea, Republic of	6.1%	0.6%
England	2.8%	3.3%
Both Parents Born Overseas	84.1%	36.7%
Both Parents Born in Australia	11.6%	51.9%
Religion		
No Religion	26.6%	17.9%
Buddhism	16.2%	2.9%
Catholic	14.6%	27.5%
Anglican	4.7%	19.9%
Hinduism	2.4%	1.7%

Indicator	Percentage	NSW Average
Language		
English Speaking Only	26.4%	72.5%
Mandarin	12.5%	2.0%
Indonesian	7.9%	0.4%
Thai	6.9%	0.2%
Cantonese	6.3%	2.0%
Korean	5.6%	0.7%
Dwelling Structure		
Separate House	2.4%	69.5%
Semi-Detached, Row or Terrace House, Townhouse	0.1%	10.7%
Flat, Unit or Apartment	97.3%	18.8%
Total Occupied Private Dwellings	81.9%	90.3%
Total Unoccupied Dwellings	18.1%	9.7%
Methods of Travel to Work		
Walk only	49.3%	4.1%
Train	12.9%	6.2%
Bus	10.5%	3.7%
Car, as driver	9.5%	57.6%
Train, bus	1.7%	1.4%
People who travelled to work by public transport	26.6%	13.8%
People who travelled to work by car as driver or passenger	11.0%	62.8%

Source: 2011 ABS Census

Infrastructure Context

The proximity and type of nearby infrastructure influences the type of people to frequent the area, the type of events and activities that can be expected in the area. This infrastructure may have an impact on the security risks that the WBAP may be directly or indirectly exposed to.

The key infrastructure nearby the WBAP includes:

- The Sydney Harbour Bridge;
- The Cahill Expressway;
- Barangaroo Headland Park;
- The Observatory;
- Roslyn Packer Theatre;
- Pier One;
- Pier 6/7 residential building;

- Pier 8;
- The Rocks;
- Circular Quay;
- Circular Quay Ferry Terminal;
- Circular Quay Train Station;
- The Overseas Passenger Terminal;
- Dawes Point Park;
- Observatory Hill Park; and
- Hickson Road Reserve.

Social Infrastructure Context

The proximity of social infrastructure to the WBAP has an impact on the consequence of security incidents that may occur.

Emergency Services

NSW Police: The WBAP is located within the Sydney City Local Area Command (LAC), within the Central Metropolitan Region. The Sydney City LAC is a 24 hour police station, and is only 2.5km from the WBAP, whilst The Rocks Police Station (also open 24/7) is only 1.5km away, enabling them to provide a quick and timely response during emergency situations.

Fire and Rescue NSW:

Fire boats are located at Pier 10 and would provide the primary response to fires within WBAP.

The Rocks Fire Station is located approximately 1.2km from the WBAP, enabling them to provide a quick and timely response during emergency situations at the WBAP.

Ambulance Service of NSW:

Paddington Ambulance Station is located approximately 5.3km from the WBAP enabling them to provide a quick and timely response during emergency situations.

Medical Services

Sydney Hospital is located approximately 2.6km from the WBAP, and St. Vincent's Hospital is located approximately 4.7km away.

The close proximity of an abundance of medical services facilities ensures that when needed, any required medical intervention at the WBAP will be able to be efficiently and effectively dealt with.

6.2.3 Socio-Economic Context

Overview

The socio-economic context looks at the socio-economic influences that may exist at or around this location. This section looks at the socio-economic status of this location.

Socio-Economic Context

Sydney has a comparatively high rate of unemployment, above average income levels, an above average representation in the Professionals occupation, an above average representation within the Food Service, Banking and Finance, Legal and IT industries, and a significantly above average number of residents who are renters.

Table 8 - Socio-Economic Context

Indicator	Percentage	NSW Average
Employment Status		
Employed – Full Time	59.5%	60.2%
Employed – Part Time	28.5%	28.2%
Away from Work	4.8%	5.7%
Unemployed	7.1%	5.9%
Total Labour Force	7,852	N/A
Occupation		
Professionals	32.9%	22.7%
Managers	14.8%	13.3%
Clerical & Administrative Workers	12.0%	15.1%
Community & Personal Services Workers	11.7%	9.5%
Sales Workers	8.8%	9.3%
Technicians & Trade Workers	8.4%	13.2%
Labourers	7.4%	8.7%
Machinery Operators & Drivers	1.0%	6.4%
Industry of Employment		
Cafes, Restaurants, & Takeaway Food Services	15.5%	4.1%
Legal and Accounting Services	5.6%	2.4%
Depository Financial Intermediation	4.7%	1.9%
Computer System Design and Related Services	4.7%	1.7%
Auxiliary Finance and Investment Services	4.4%	1.3%
Median Incomes (Weekly)		
Personal	$639	$561
Family	$1,658	$1,477

Indicator	Percentage	NSW Average
Household	$1,436	$1,237
Housing Tenure		
Owned Outright	16.0%	33.2%
Owned with a Mortgage	17.7%	33.4%
Rented	63.4%	30.1%
Dwelling Structure		
Separate House	2.4%	69.5%
Semi-Detached, Row or Terrace House, Townhouse	0.1%	10.7%
Flat, Unit or Apartment	97.3%	18.8%
Total Occupied Private Dwellings	81.9%	90.3%
Total Unoccupied Dwellings	18.1%	9.7%
Methods of Travel to Work		
Walk only	49.3%	4.1%
Train	12.9%	6.2%
Bus	10.5%	3.7%
Car, as driver	9.5%	57.6%
Train, bus	1.7%	1.4%
People who travelled to work by public transport	26.6%	13.8%
People who travelled to work by car as driver or passenger	11.0%	62.8%

Source: 2011 ABS Census

As mentioned above, Sydney has above average income levels, with the median personal income 13.9% higher than the state median, but also has a high rate of unemployment at 7.1%, compared to the state unemployment rate of 5.9%. Sydney has above average representation in the Professionals, and Community & Personal Services Workers professions, and below average representation in the machinery operators & drivers, and Technicians & Trade Workers professions. Sydney has above average representation within the Food Service, Banking and Finance, Legal and IT industries.

6.2.4 Market Context

Overview

The market context helps define unique risks that may be present within the market that the organisation operates, or within the key local, state, or national markets where the organisation is located.

Organisation Market and Competition

The WBAP is an arts and cultural precinct, and as such competes with other prominent Sydney arts and cultural facilities for patrons, events, acts, and public and private funding. A number of the WBAP tenants do also hold their events and performances at these other cultural facilities.

Suburb Markets

The suburb of Sydney covers the central business district (CBD). The Sydney CBD is Australia's main financial centre, as well as being one of the main economic hubs within the Asia-Pacific region.

The Sydney CBD is home to some of the largest Australian companies, as well as serving as an Asia-Pacific headquarters for many large international companies.

The type, size and make-up of a market has a significant impact on an areas' security risk profile.

State Markets

Services account for 86% of the value of New South Wales' industry output, highlighting the strength of the state's knowledge-based business services, ICT and creative industries.

The state dominates the nation's financial and insurance services, professional, scientific and technical services, and information media and telecommunications industries, as well as the tourism-related accommodation and food services, and arts and recreation services industries.

With the exception of the construction industry, all NSW services industries are the largest in Australia.

Financial and insurance services is the state's largest industry, accounting for a 12% share of the New South Wales economy in 2012-13. Concentrated in Sydney, Australia's business and finance capital, this industry has increased its share of GSP by more than four percentage points over the last 20 years.

Demonstrating its economic diversity, NSW contributes the largest state share of national output not only in services (33%) but also in manufacturing (34%).

NSW has particular strengths in food product manufacturing, primary metal and metal product manufacturing, and machinery and equipment manufacturing.

National Markets

Australia has a diversified, services based economy, with the services sector (excluding construction) accounting for more than 70 per cent of real gross value added (GVA). The country's sophisticated financial services industry is the largest contributor to its economy, generating 9.3 per cent of total GVA. Professional, scientific and technical services, education and training, and information media and telecommunications together make up almost 15 per cent of total output, reflecting Australia's highly skilled, well-educated and innovative workforce.

The Australian economy is estimated to be the 12th largest in the world in 2015, despite the fact the country is home to only 0.3 per cent of the world's population.

Australia's nominal GDP is estimated at US$1.2 trillion and accounts for 1.7 per cent of the global economy. Australia has almost doubled the value of its total production from a decade ago.

Australia continues to see strong annual growth in key industries, including information media and telecommunications, financial and insurance services, construction, and professional, scientific and technical services. Overall, Australia's services sector has expanded by an average of 3.3 per cent per annum.

Australia is globally successful in five significant and diverse sectors: agribusiness, education, tourism, mining and wealth management.

Australia is ranked in the top 14 countries globally for agricultural product exports, 3rd for foreign students in tertiary education, 11th for international tourism, top 5 for fuel and mining exports, and Australia has the 7th largest investment fund assets pool.

Australia has the world's largest share of iron ore, gold, zinc, nickel and uranium reserves.

6.2.5 Geopolitical Context

Overview

The geopolitical context details the major current geopolitical issues that may affect the WBAP directly, or indirectly as part of the wider community and society. The geopolitical context also looks at how politically stable the areas/countries that WBAP operates and/or resides in are, and what terrorist or organised crime groups operate in these areas/countries.

Local Political Context

The WBAP is located within the suburb of Sydney, which falls within the City of Sydney Local Government Area (LGA), and the State Electorate of Sydney. The State Electorate of Sydney is currently held by an Independent party.

The current NSW state government is the Coalition (Liberal Party of Australia, and the National Party of Australia).

The suburb of Sydney falls within the Federal Division of Sydney. The Federal Division of Sydney is a safe Labor Party seat.

The current federal government is the Coalition (Liberal Party of Australia, and the National Party of Australia).

Australian Geopolitical Context

Quality of Government

The quality of governance in Australia ranks among the best in the world, ranked 10th by the World Bank, Worldwide Governance Indicators 2015.

Political Stability

The Economist Political Instability Index (2009-2010) rates Australia as the 11th most politically stable country, out of 165 countries ranked. The Political Instability Index shows the level of threat posed to governments by social protest. The index scores are derived by combining measures of economic distress and underlying vulnerability to unrest.

Level of Peace

The 2015 Global Peace Index produced by the Institute for Economics & Peace, ranked Australia as the 9th most peaceful country. The index gauges global peace using three broad themes:

- The level of safety and security in society;
- The extent of domestic and international conflict; and
- The degree of militarisation.

Level of Terrorism

The 2015 Global Terrorism Index produced by the Institute for Economics & Peace, accounts for the direct and indirect impact of terrorism in 162 countries in terms of its effect on lives lost, injuries, property damage and the psychological after-effects of terrorism. This Index ranked Australia the 59th most impacted country.

Organised Crime

Organised crime groups engineer much of Australia's serious crime. These groups are often well-planned enterprises focused on making money. They are capable, resourceful and resilient and are engaged in a wide range of activity across many sectors and at all levels of society.

The Australian Crime Commission conservatively estimates that serious and organised crime costs Australia $15 billion every year. This cost comprises loss of business and taxation revenues, expenditure on law enforcement and regulatory efforts, and social and community impacts of crime.

Outlaw motorcycle gangs (OMCGs) remain one of the most high profile manifestations of organised crime in Australia. They have an active presence in all Australian states and territories.

OMCG activities are mostly domestic. However, there is an increasing prevalence of international connections, with gangs cooperating with other chapters overseas and with sophisticated and high-threat organised crime groups operating in Australia and internationally.

The most recent assessment of OMCGs identified that there are more than 40 OMCGs operating in Australia, with about 6000 patched members. The total club and membership numbers of Australian OMCGs is rising.

In addition to OMCG's, a number of international mafia's (Italian, Serbian, Albanian, Russian, Japanese etc.) have local representation, as do international drug cartels, and there is also a number of local and international East and South-East Asian gangs present. In NSW, there is a particular concern about Middle

Eastern organised crime groups, as evident by the Middle Eastern Organised Crime Squad, within the NSW Police Force.

The Australian Crime Commission also estimates that approximately 70 per cent of Australia's serious and organised crime threats are based offshore.

The WBAP is not considered a legitimate target for organised crime.

Regional Geopolitical Context

As China rises, geopolitical risk across Asia & the Pacific will inevitably grow. But not this year. The region's top leaders, Japan's Shinzo Abe (hosting the Group of Seven meeting this year), India's Narendra Modi, and especially China's Xi (hosting the Group of 20), are now focused on stabilising big power relations in the Asia-Pacific region, not stoking tensions. With the entire regional economy slowing, it will be a year of more stimulus at home, less actions abroad. The opposite of Europe, where eroding political capital fosters insecurity, Asia's most worrisome conflicts are buffered by leaders who can focus on their top priorities.

And so despite plenty of tensions in the South China Sea—and continued posturing over Chinese-made artificial islands in that area—there's a limit to how far confrontation can go in 2016. So too China-Japan and South Korea-Japan relations, where none of the feuding governments are prepared to escalate the sort of political, diplomatic, or commercial conflict that might be bad for business. The exceptions are Taiwan and Hong Kong, considered internal issues by Beijing, and bringing little pushback from other powers. Indeed, the politics could be sufficiently strong to bring progress in conflicts historically seen as unyielding, raising the possibility, for example, that a politically unthreatened Putin could offer a deal for cash in Russia's longstanding territorial conflict with Japan. Even more dramatically, the personally uncontainable Modi (India) could throw his weight behind breaking his country's diplomatic impasse with Pakistan. **Source: Top Political Risks 2016 - Eurasia Group**

6.3 Internal Context

6.3.1 Overview

The focus of developing the internal context is to create an agreed understanding of the WBAP internal environment and issues that may influence the nature of the security risk exposures or the activities being undertaken to manage them.

6.3.2 Organisation Overview

Any security risk management activity must be conducted within the parameters of the organisation's context. The objectives for security risk management must be aligned with the organisation's objectives and be supportive of the manner in which the organisation conducts itself.

Organisation

Arts NSW is the primary organisation responsible for the operation of the WBAP. Arts NSW is the NSW Government's arts and culture policy and investment body.

Arts NSW invest in the success and future of arts and culture in NSW through their infrastructure and funding programs, and targeted strategies. Arts NSW work collaboratively with the NSW cultural institutions, the arts and cultural sector and partners within government. Arts NSW make opportunities for more people to shape and experience the arts.

Tenants

The key tenants at the WBAP will include:

- Sydney Theatre Company;
- Sydney Dance Company;
- Australian Theatre for Young People (ATYP);
- Bangarra Dance Theatre;
- Australian Chamber Orchestra (ACO);
- Bell Shakespeare Company;
- Philharmonia Choirs;
- Gondwana Choirs; and
- The Song Company.

6.3.3 Critical Assets

The critical assets of the WBAP will include, but are not limited to the following:

- Utility infrastructure;
- Performance and event spaces such as the Wharf Theatres, ATYP Theatre, and the ACO Auditorium; and
- Large rehearsal spaces for Bell Shakespeare, Bangarra, and Sydney Dance Company.

6.3.4 Critical Functions

The critical functions provided by the WBAP include, but are not limited to the following:

- Holding Art and cultural events, performances, and festivals.

6.3.5 SRA Exclusions

This SRA has been limited to Pier 2/3, Wharf 4/5, and the waterfront public square, and has excluded the other Walsh Bay facilities and areas.

7 Risk Identification

7.1 Overview

Risk identification is concerned with creating a well thought out and comprehensive determination of the sources of risks and potential events that will have an impact upon the organisation's objectives. In undertaking risk identification, the following should and will be considered:

- How a security risk could happen (source of risk);
- What could happen (the potential risk event);
- Where it could happen; and
- Who could be involved (specific individuals or groups).

7.2 Threat Sources

7.2.1 Overview

For security risks, there are generally three broad sources of risk – criminal, malicious, or terrorist threats.

7.2.2 Criminal Threats

Criminal threats are usually driven by personal gain and are targeted at gaining control of attractive assets. This could include fraud, theft, sabotage, extortion, kidnap and ransom.

7.2.3 Malicious Threats

Malicious threats include activities such as vandalism, sabotage, unauthorised information disclosure, IT attacks, harassment, assault, etc. A malicious act is usually a specific direct attack on the targeted organisation and is often motivated by revenge, fame, association or challenge. Sources include disgruntled or disturbed current or former employees, contractors, customers, or community protestors. More general threats such as circulating malware (viruses, Trojans, worms, etc.) are equally valid considerations.

7.2.4 Terrorism Threats

There is no internationally accepted definition of terrorism. One comprehensive definition describes terrorism as: 'act of terrorism means an act, including but not limited to the use of force or violence on, or the threat thereof, of any person or group(s) of persons, whether acting alone, or on behalf of or in connection with the organisation(s) or government(s), which from its nature or context is done for, or in connection with, political, religious, ideological, ethnic or similar purposes

or reasons, including the intention to influence any government and/or to put the public, or any section of the public, in fear'.

7.3 Risk Impact Categories

7.3.1 Overview

Each identified security risk will impact the WBAP in at least one of the following ways.

7.3.2 Business Continuity

A security risk, should it materialise may affect the continuity of business. Business Continuity refers to the capability of the organisation to continue the delivery of its products or services at acceptable predefined levels.

7.3.3 Liability

The WBAP may be legally responsible for the consequences of a security risk, should it materialise.

7.3.4 Financial

A security risk, should it materialise may cost the WBAP financially.

7.3.5 Safety

A security risk, should it materialise may negatively affect the safety of staff, contractors or the general public.

7.3.6 Infrastructure, Assets and Systems

A security risk, should it materialise may negatively affect the WBAP's infrastructure, assets or systems.

7.3.7 Political

The materialisation of a security risk may have political consequences for the WBAP.

7.3.8 Reputation

The materialisation of a security risk may negatively affect the reputation of the WBAP.

7.4 Identified Security Risks

The identified security risks that the WBAP is exposed to are listed below, along with the security risk impact, risk impact category, and an identification of existing controls.

Table 9 - Identified Security Risks

Threat Source	Security Risk	Security Risk Event	Security Risk Impact	Risk Impact Category	Identification of Existing Controls
Malicious Threat	Assault	Assault of patrons within public realm	Impact to safety, patron experience, damage to reputation	Safety	Lighting CCTV
Malicious Threat	Assault	Assault of patrons within waterfront square	Impact to safety, patron experience, damage to reputation	Safety	N/A
Malicious Threat	Assault	Assault of patrons within Pier 2/3, Wharf 4/5 commercial/function spaces	Impact to safety, patron experience, damage to reputation	Safety	EACS to control access into building. CCTV within building
Malicious Threat	Assault	Assault of patrons within bar at the end of the wharf	Impact to safety, patron experience, damage to reputation	Safety	EACS to control access into building. CCTV within building
Malicious Threat	Assault	Assault of staff within public realm	Impact to safety, staff experience, damage to reputation	Safety	Lighting CCTV
Malicious Threat	Assault	Assault of staff within waterfront square	Impact to safety, staff experience, damage to reputation	Safety	N/A
Malicious Threat	Assault	Assault of staff within Pier 2/3, Wharf 4/5 commercial/function spaces	Impact to safety, staff experience, damage to reputation	Safety	EACS to control access into building. CCTV within building
Malicious Threat	Assault	Assault of staff at box office/reception desks/concierge	Impact to safety, staff experience, damage to reputation	Safety	EACS to control access into building. CCTV within building
Malicious Threat	Assault	Assault of staff within bar at the end of the wharf	Impact to safety, staff experience, damage to reputation	Safety	EACS to control access into building. CCTV within building
Malicious Threat	Assault	Assault of staff at Level 1 Pier 2/3 bar	Impact to safety, staff experience, damage to reputation	Safety	EACS to control access into building. CCTV within building
Malicious Threat	Assault	Assault of patrons at Level 1 Pier 2/3 bar	Impact to safety, patron experience, damage to reputation	Safety	EACS to control access into building. CCTV within building
Malicious Threat	Assault	Indecent assault of patrons within public realm	Impact to safety, patron experience, damage to reputation	Safety	Lighting CCTV
Malicious Threat	Assault	Indecent assault of patrons within WBAP buildings	Impact to safety, patron experience, damage to reputation	Safety	EACS to control access into building. CCTV within building

Threat Source	Security Risk	Security Risk Event	Security Risk Impact	Risk Impact Category	Identification of Existing Controls
Malicious Threat	Assault	Indecent assault of staff within public realm	Impact to safety, staff experience, damage to reputation	Safety	Lighting CCTV
Malicious Threat	Assault	Indecent assault of staff within WBAP buildings	Impact to safety, staff experience, damage to reputation	Safety	EACS to control access into building. CCTV within building
Criminal Threat	Theft	Theft from café	Financial loss, impact to reputation	Financial	EACS to control access into building. CCTV within building
Criminal Threat	Theft	Theft from commercial/function spaces	Financial loss, impact to reputation	Financial	EACS to control access into building. CCTV within building
Criminal Threat	Theft	Theft from cleaners store room	Financial loss, impact to reputation	Financial	EACS to control access into building. CCTV within building
Criminal Threat	Theft	Theft from merchandise store	Financial loss, impact to reputation	Financial	EACS to control access into building. CCTV within building
Criminal Threat	Theft	Theft from store rooms	Financial loss, impact to reputation	Financial	EACS to control access into building. CCTV within building
Criminal Threat	Theft	Theft from office areas	Financial loss, impact to reputation	Financial	EACS to control access into building. CCTV within building
Criminal Threat	Theft	Theft from box office/cloak room	Financial loss, impact to reputation	Financial	EACS to control access into building. CCTV within building
Criminal Threat	Theft	Theft from bar store	Financial loss, impact to reputation	Financial	EACS to control access into building. CCTV within building
Criminal Threat	Theft	Theft from Level 1 pier 2/3 bar	Financial loss, impact to reputation	Financial	EACS to control access into building. CCTV within building
Criminal Threat	Theft	Theft from bar at the end of the wharf	Financial loss, impact to reputation	Financial	EACS to control access into building. CCTV within building
Criminal Threat	Theft	Theft of vehicles	Financial loss, impact to reputation	Financial	Lighting CCTV
Criminal Threat	Theft	Theft from vehicles	Financial loss, impact to reputation	Financial	Lighting CCTV
Criminal Threat	Robbery / Steal from person	Robbery/steal from staff within public realm/waterfront square	Impact to safety, staff experience, damage to reputation, financial loss	Safety	Lighting CCTV
Criminal Threat	Robbery / Steal from person	Robbery/steal from patrons within public realm/waterfront square	Impact to safety, patron experience, damage to reputation, financial loss	Safety	Lighting CCTV
Criminal Threat	Robbery / Steal from person	Robbery/steal from staff within WBAP buildings	Impact to safety, staff experience, damage to reputation, financial loss	Safety	EACS to control access into building. CCTV within building

Threat Source	Security Risk	Security Risk Event	Security Risk Impact	Risk Impact Category	Identification of Existing Controls
Criminal Threat	Robbery / Steal from person	Robbery/steal from patrons within with in WBAP buildings	Impact to safety, patron experience, damage to reputation, financial loss	Safety	EACS to control access into building. CCTV within building
Malicious Threat	Vandalism	Malicious damage/graffiti of WBAP buildings	Property/asset damage	Infrastructure, Assets & Systems	EACS to control access into building. CCTV within building
Malicious Threat	Vandalism	Malicious damage/graffiti of public realm infrastructure & assets	Property/asset damage	Infrastructure, Assets & Systems	Lighting CCTV
Malicious Threat	Vandalism	Malicious damage/graffiti within WBAP buildings	Property/asset damage	Infrastructure, Assets & Systems	EACS to control access into building. CCTV within building
Malicious Threat	Antisocial Behaviour	Harassment, threatening behaviour, public nuisance, offensive conduct within public realm	Impact to safety, staff/patron experience, damage to reputation	Safety	Lighting CCTV
Malicious Threat	Antisocial Behaviour	Harassment, threatening behaviour, public nuisance, offensive conduct within WBAP buildings	Impact to safety, staff/patron experience, damage to reputation	Safety	EACS to control access into building. CCTV within building
Malicious Threat	Antisocial Behaviour	Drug use and/or possession within public realm	Impact to safety, staff/patron experience, damage to reputation	Safety	Lighting CCTV
Malicious Threat	Antisocial Behaviour	Drug use and/or possession within WBAP buildings	Impact to safety, staff/patron experience, damage to reputation	Safety	EACS to control access into building. CCTV within building
Malicious Threat	Antisocial Behaviour	Drug dealing within public realm	Impact to safety, staff/patron experience, damage to reputation	Reputation	Lighting CCTV
Malicious Threat	Antisocial Behaviour	Drug dealing within WBAP buildings	Impact to safety, staff/patron experience, damage to reputation	Reputation	Lighting CCTV
Malicious Threat	Antisocial Behaviour	Intoxicated persons within public realm	Impact to safety, staff/patron experience, damage to reputation	Safety	EACS to control access into building. CCTV within building
Malicious Threat	Antisocial Behaviour	Intoxicated persons within Level 1 pier 2/3 bar	Impact to safety, staff/patron experience, damage to reputation	Safety	EACS to control access into building. CCTV within building

Threat Source	Security Risk	Security Risk Event	Security Risk Impact	Risk Impact Category	Identification of Existing Controls
Malicious Threat	Antisocial Behaviour	Intoxicated persons within Bar at the end of the wharf	Impact to safety, staff/patron experience, damage to reputation	Safety	EACS to control access into building. CCTV within building
Malicious Threat	Antisocial Behaviour	Intoxicated persons within commercial/function spaces	Impact to safety, staff/patron experience, damage to reputation	Safety	EACS to control access into building. CCTV within building
Criminal Threat	Trespass	Break & enter into WBAP buildings	Safety issues, unauthorised access to assets	Financial	EACS to control access into building. CCTV within building
Criminal Threat	Trespass	Unauthorised access to back of house areas	Safety issues, unauthorised access to assets	Financial	EACS to control access into building. CCTV within building
Criminal Threat	Trespass	Break & enter/unauthorised access into plant areas	Safety issues, unauthorised access to assets	Safety	EACS to control access into building. CCTV within building
Criminal Threat	Trespass	Break & enter into commercial areas	Safety issues, unauthorised access to assets	Financial	EACS to control access into building. CCTV within building
Criminal Threat	Trespass	Unauthorised access to office areas	Safety issues, unauthorised access to assets	Financial	EACS to control access into building. CCTV within building
Malicious Threat	Murder / Attempted Murder	Within public realm	Impact to safety, damage to reputation	Safety	Lighting CCTV
Malicious Threat	Murder / Attempted Murder	Within WBAP buildings	Impact to safety, damage to reputation	Safety	EACS to control access into building. CCTV within building
Malicious Threat	Arson	Deliberate act to damage facilities or to disrupt operations	Damage to assets, chance of injuries, disruption to operations	Business Continuity	EACS to control access into building. CCTV within building
Malicious Threat	Arson	Deliberate act to damage public realm infrastructure or to disrupt operations	Damage to assets, chance of injuries, possible disruption to operations	Infrastructure, Assets & Systems	Lighting CCTV
Malicious Threat	Protest / Demonstration	Protest or demonstration by Issue Motivated Groups resulting in illegal occupation of the public realm, unwanted media exposure, interruption to operations, etc.	Impact to safety, damage to reputation, disruption to operations	Political	Lighting CCTV
Malicious Threat	Protest / Demonstration	Protest or demonstration by Issue Motivated Groups resulting in illegal	Impact to safety, damage to reputation, disruption to operations	Political	EACS to control access into building. CCTV within building

Threat Source	Security Risk	Security Risk Event	Security Risk Impact	Risk Impact Category	Identification of Existing Controls
		occupation of the WBAP buildings, unwanted media exposure, interruption to operations, etc.			
Criminal Threat	Abduction / Kidnapping	From within public realm	Impact to safety, damage to reputation, disruption to operations	Safety	Lighting CCTV
Criminal Threat	Abduction / Kidnapping	From within WBAP buildings	Impact to safety, damage to reputation, disruption to operations	Safety	EACS to control access into building. CCTV within building
Terrorism Threat	Hostage / Siege	Within public realm	Impact to safety, damage to reputation, disruption to operations	Safety	Lighting CCTV
Terrorism Threat	Hostage / Siege	Within performance / function / event spaces	Impact to safety, damage to reputation, disruption to operations	Safety	EACS to control access into building. CCTV within building
Terrorism Threat	Hostile Vehicle attack	Within public realm	Impact to safety, damage to reputation, disruption to operations	Safety	Lighting CCTV Bollards Roller shutters
Terrorism Threat	Placed / Person Borne IED	Within waterfront square	Impact to safety, damage to reputation, disruption to operations	Safety	N/A
Terrorism Threat	Placed / Person Borne IED	Within performance / function / event spaces	Impact to safety, damage to reputation, disruption to operations	Safety	EACS to control access into building. CCTV within building
Terrorism Threat	Vehicle Borne IED	Within public realm	Impact to safety, damage to reputation, disruption to operations	Safety	Lighting CCTV Bollards Roller shutters
Terrorism Threat	Knife attack	Within public realm	Impact to safety, damage to reputation, disruption to operations	Safety	Lighting CCTV
Terrorism Threat	Knife attack	Within waterfront square	Impact to safety, damage to reputation, disruption to operations	Safety	N/A
Terrorism Threat	Knife attack	Within performance / function / event spaces	Impact to safety, damage to reputation, disruption to operations	Safety	EACS to control access into building. CCTV within building
Terrorism Threat	Active shooter	Within public realm	Impact to safety, damage to reputation, disruption to operations	Safety	Lighting CCTV
Terrorism Threat	Active shooter	Within waterfront square	Impact to safety, damage to reputation, disruption to operations	Safety	N/A
Terrorism Threat	Active shooter	Within performance / function / event spaces	Impact to safety, damage to reputation, disruption to operations	Safety	EACS to control access into building. CCTV within building

Threat Source	Security Risk	Security Risk Event	Security Risk Impact	Risk Impact Category	Identification of Existing Controls
Terrorism Threat	CBR attack	Within public realm	Impact to safety, damage to reputation, disruption to operations	Safety	Lighting CCTV
Terrorism Threat	CBR attack	Within waterfront square	Impact to safety, damage to reputation, disruption to operations	Safety	N/A
Terrorism Threat	CBR attack	Within performance / function / event spaces	Impact to safety, damage to reputation, disruption to operations	Safety	EACS to control access into building. CCTV within building

7.5 Security Risk Events – Criminal and Malicious

The following is a list of the most prevalent crimes to occur in the City of Sydney LGA that are relevant to the WBAP, based on total number of offences. A ranking of how the City of Sydney LGA crime rates compares to the other 141 LGA's cannot be provided because its residential population does not accurately reflect the number of people present in the area each day.

1. Theft (Other) (3,948 offences);
2. Assault – non-domestic violence related (3,121 offences);
3. Possession and/or use of cannabis (3,045 offences);
4. Malicious damage to property (2,691 offences);
5. Steal from motor vehicle (1,686 offences);
6. Steal from person (1,661 offences);
7. Possession/Use of amphetamines (1,265 offences);
8. Offensive conduct (1,126 offences);
9. Possession and/or use of ecstasy (1,055 offences); and
10. Harassment, threatening behaviour and public nuisance (943 offences).

Source: BOCSAR

The top offences to occur within an Outdoor/Public Place setting within the Sydney LGA were:

1. Assault – non-domestic violence related (1,213 offences);
2. Steal from motor vehicle (1,028 offences).
3. Malicious damage to property (753 offences);
4. Steal from person (453 offences);
5. Motor vehicle theft (235 offences);
6. Robbery (225 offences);
7. Assault –domestic violence related (175 offences);
8. Sexual offences (115 offences); and

9. Break and enter non-dwelling (1 offence).

Source: BOCSAR

Note: Premises type data is not collected for all offence categories.

7.6 Security Risk Events – Terrorism

The terrorism based security risks relevant to the WBAP include the following:

- Person Borne Improvised Explosive Device (PBIED) / Placed IED;
- Vehicle Borne Improvised Explosive Device (VBIED);
- Hostile Vehicle Attack;
- Active Shooter;
- Knife Attack;
- Hostage / Siege Scenario; and
- Chemical / Biological / Radiological Attack (CBR).

8 Risk Analysis

8.1 Overview

The aim of undertaking risk analysis is to:

- Determine the adequacy and appropriateness of existing controls to manage identified priority risks;
- Prioritise risks for subsequent evaluation of tolerance or need for further treatment; and
- Provide an improved understanding of the vulnerability of critical assets to identified risks.

The output of this analysis should, through the evaluation step, provide decision makers with sufficient information to make an informed decision on the need for increasing or decreasing the investment being made for protection across the spectrum of assets under consideration.

8.2 Analysis of Total Security Risks

The security risk assessment process has assessed the security risk profile of the WBAP and has identified 72 security risks.

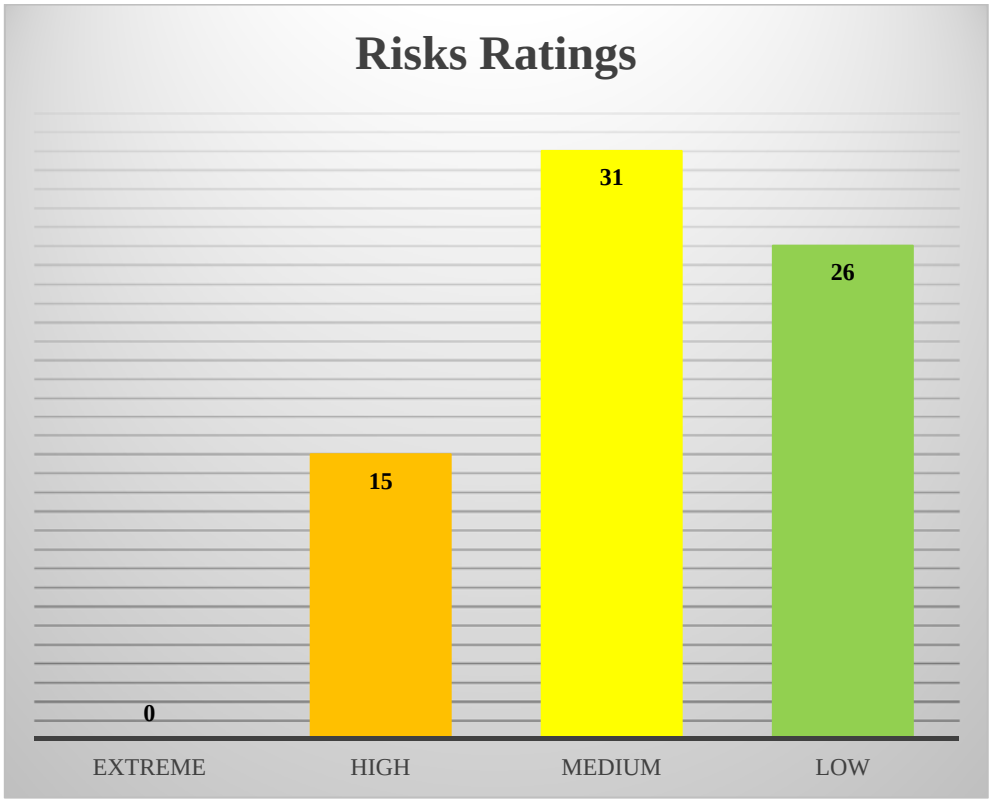


Figure 2 – Security Risk Ratings

As can be seen in the figure above, of the 72 identified security risks, 0 were assessed as Extreme, 15 were assessed as High, 31 were assessed as Medium, and 26 were assessed as Low.

It should be noted that all 15 High risks are terrorist based risks, and all of their likelihood of occurrence have been assessed as Rare or Unlikely, however their High risk rating is due to their potential Catastrophic consequence.

Ten of the 22 Medium security risks have a likelihood rating of Almost Certain or Likely, but a consequence rating of Minor or Minimal, which are the two lowest consequence ratings. Therefore any proposed security treatment measures should focus on reducing their likelihood of occurrence.

Only 15 of the 72 total security risks identified have consequence ratings of Moderate or above, and all 15 have likelihood ratings of Rare or Unlikely. Therefore any proposed security treatment measures should focus on reducing their consequence rating.

Importantly, **NONE** of the identified security risks are both high consequence and high likelihood risks (Catastrophic, Major or Moderate, and Almost Certain, Likely, or Possible). This means that all of the identified security risks are either high consequence but low likelihood, or high likelihood but low consequence events. These risks are therefore more tolerable.

Based on the outcome of the security risk assessment, all identified security risks can be tolerated if it is not reasonably practicable to reduce the risk further. However, if there are options for further risk reduction and the cost is proportionate to the benefits to be gained, then implementation of these measures should be considered.

8.3 Analysis of Crime and Malicious Based Risks

8.3.1 Overview

A ranking of how the City of Sydney LGA crime rates compares to the other 141 LGA's cannot be provided because its residential population does not accurately reflect the number of people present in the area each day. Due to the large number of people who frequent the CBD each day, the Sydney LGA generally has a high rate of crime.

The premises type most applicable to the WBAP is an Outdoor/Public Place type premises, therefore this premises type will be used in the analysis that follows.

The following statistics are based on the 2015 recorded crime statistics compiled by BOCSAR.

8.3.2 State-Wide Crime Trends

In the 24 months to June 2016, two of the 17 major offences showed a significant upward trend across NSW, nine were trending downward and the remaining six

offences were stable. The offences trending upward were steal from retail store (up 6.3%) and fraud (up 1.7%).

The nine offences trending down, over the previous 24 months were:

- Murder (down 32.1%);
- Robbery without a weapon (down 25.9%);
- Robbery with a firearm (down 41.7%);
- Robbery with a weapon not a firearm (down 22.2%);
- Break and enter dwelling (down 7.2%);
- Motor vehicle theft (down 12.6%);
- Steal from dwelling (down 6.6%);
- Steal from person (down 9.9%); and
- Malicious damage to property (down 3.2%).

The changes mentioned above over the previous 24 months now mean that 12 major categories of crime in NSW are now at their lowest level in 20 years.

The 12 major crime categories at 20 year lows are:

- Murder;
- Robbery without a weapon;
- Robbery with a firearm;
- Robbery with a weapon not a firearm;
- Break and enter dwelling;
- Break and enter non-dwelling;
- Motor vehicle theft;
- Steal from motor vehicle;
- Steal from retail store;
- Steal from dwelling;
- Steal from person; and
- Malicious damage to property.

Shootings (not a major crime category) are also at the lowest level in 20 years.

8.3.3 Five Year LGA Crime Trend

As can be seen in the five year crime trend table below, seven of the 10 most prevalent offences applicable to the WBAP have reduced in occurrence over the

previous three and five year periods. Out of the 10 most prevalent offences, only drug offences have risen over the three and five year periods.

Based on these trends, the likelihood of these seven offences occurring in the future should generally either remain the same as currently assessed, or reduce.

Table 10 - Five Year Trend Table

Offence	Jan to Dec 11	Jan to Dec 12	Jan to Dec 13	Jan to Dec 14	Jan to Dec 15	3 Year Change	5 Year Change
Other Theft	5110	5379	4880	4692	3948	-19.10%	-22.74%
Assault – non-domestic violence related	3772	3724	3576	3142	3121	-12.72%	-17.26%
Possession and / or use of cannabis	2652	2548	2448	2714	3045	24.39%	14.82%
Malicious damage to property	3599	3332	3343	2876	2691	-19.50%	-25.23%
Steal from motor vehicle	2713	2200	2351	2176	1686	-28.29%	-37.85%
Steal from person	2881	2736	2225	1887	1661	-25.35%	-42.35%
Possession and / or use of amphetamines	2652	2548	2448	2714	3045	24.39%	14.82%
Offensive conduct	1860	1682	1713	1318	1126	-34.27%	-39.46%
Possession and / or use of ecstasy	579	915	929	949	1055	13.56%	82.21%
Harassment, threatening behaviour and public nuisance	973	1023	1025	950	939	-8.39%	-3.49%

Source: BOCSAR

General statistical information related to crime types was sourced from BOCSAR relating to crime incidents that have occurred in the City of Sydney LGA. These statistics are not detailed to suburb or street level and therefore they may not provide a complete representation of historic incidents at the WBAP.

8.3.4 Theft Offences

Risk Rating

Theft offences have been assessed as **Low** to **Medium** risks. Theft risks assessed as **Medium** have generally be done so due to their assessed Likely Likelihood.

Crime Statistics

Theft (other) is the most prevalent offence type to occur within the Sydney LGA.

Crime Hot Spots

Crime hot spots are not available for this offence category.

Risk Analysis

Premises type, victim, offender, alcohol related, and time of offence data for theft (other) offences is not recorded by BOCSAR.

The number of theft (other) offences have decreased by 22.74% over the past five years, and have decreased by 19.10% over the past 3 years. If these trends continue, it is likely that the risks posed to the WBAP by this offence type will continue to decrease.

8.3.5 Non-Domestic Violence Related Assaults

Risk Ratings

Non-domestic violence related assaults have been assessed as **Medium** to **Low** risks, primarily due to their assessed Minimal consequence ratings.

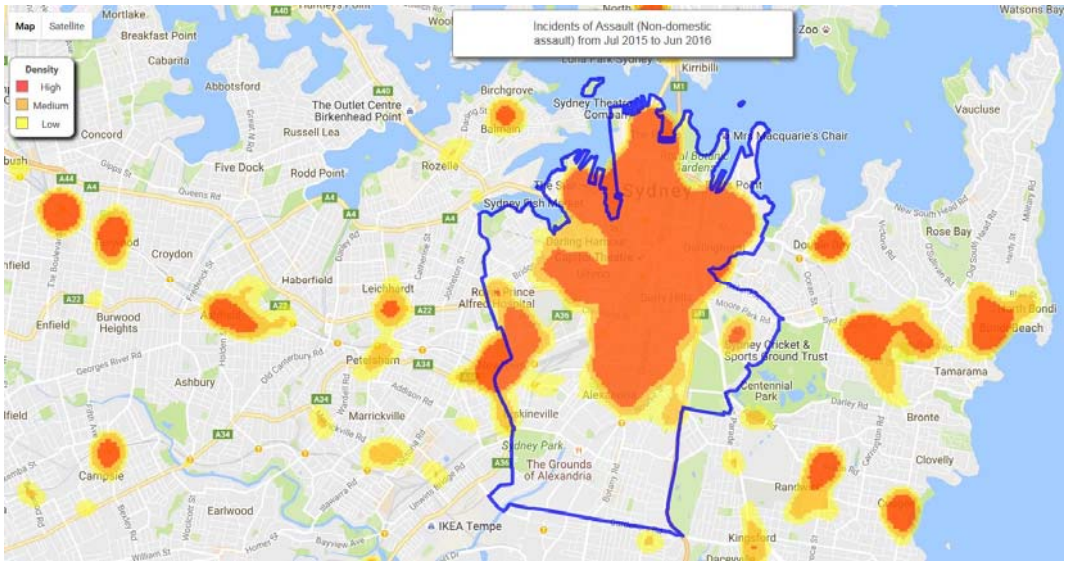
Crime Statistics

Non-domestic violence related assaults are the second most prevalent offence type to occur within the Sydney LGA, and the most prevalent offence category within Outdoor/Public Place settings.

Crime Hot Spots

The maps below portrays the non-domestic assault hotspots for the entire City of Sydney LGA:

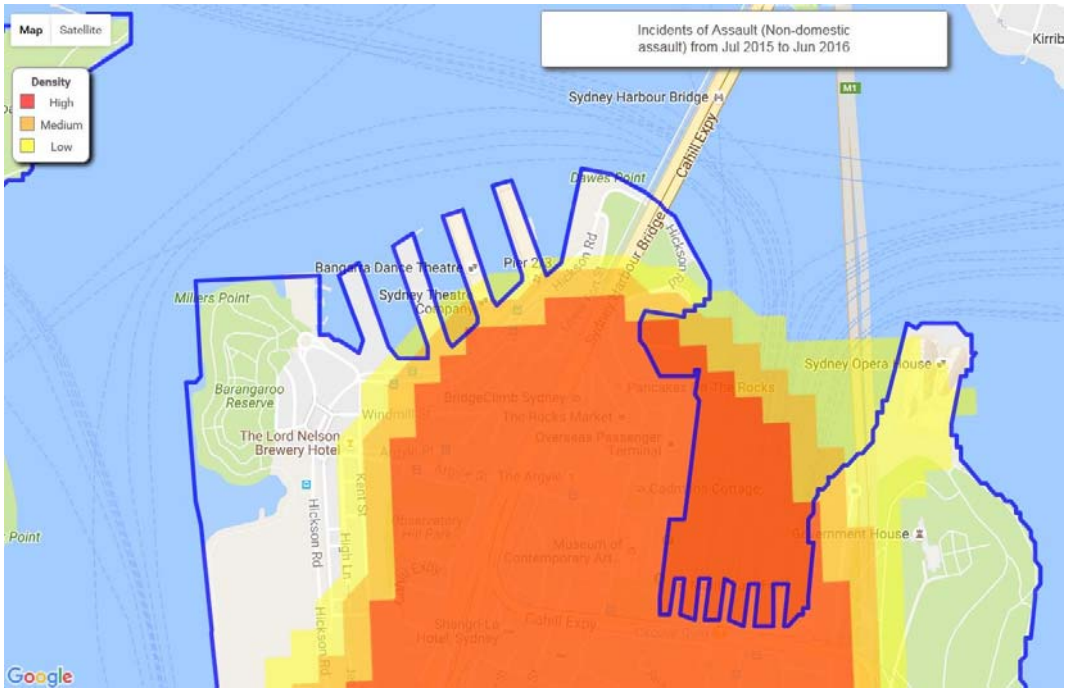
Figure 3 – Sydney LGA Assault Hotspot



Source: BOCSAR

The map below portrays the non-domestic assault hotspots for the WBAP area:

Figure 4 - WBAP Area Assault Hotspot



Source: BOCSAR

As can be seen in the maps above, the assault hot spot covers most of the Sydney LGA, however it is less prevalent within the WBAP, with only a low density of offences occurring in some of this area.

Risk Analysis

Non-domestic violence related assaults are the second most prevalent offence type to occur within the Sydney LGA, and the most prevalent offence category within

Outdoor/Public Place settings. Of the 3,121 non-domestic violence related assaults, 1,213 were recorded in an Outdoor/Public Place setting within the Sydney LGA during 2015.

The victims of non-domestic related assault offences within the Sydney LGA are most likely to be men aged 18-29. Those most likely to commit non-domestic related assault offences within the Sydney LGA are men aged 20-29. 49.3% of assault offences were recorded as alcohol related.

Non-domestic violence related assault is most likely to occur within the Sydney LGA on a Sunday morning between 12 – 6am.

The number of non-domestic related assault offences has decreased by 17.26% over the previous 5 years, and decreased by 12.72% over the last 3 years within the Sydney LGA, making it likely that the risks posed to the WBAP by this offence type will continue to reduce.

8.3.6 Drug Offences

Risk Rating

Drug offences have been assessed as **Medium** to **Low** risks. The **Medium** risk rating is due to the assessed Likely likelihood.

Crime Statistics

Drug offences are the third, seventh, and the ninth most prevalent offence types to occur within the Sydney LGA.

Crime Hot Spots

Crime hot spots are not available for this offence category.

Risk Analysis

Premises type, victim, offender, alcohol related, and time of offence data for harassment, threatening behaviour and public nuisance offences is not recorded by BOCSAR.

The number of all three drug offence categories have increased by between 14.82% and 82.21% over the past five years, and by 13.56% and 24.39% over the last 3 years within the Sydney LGA, making it likely that the risks posed to the WBAP by these offence types will continue to rise in the future.

8.3.7 Malicious Damage to Property Offences

Risk Rating

Malicious damage/graffiti to property, infrastructure, or assets has been assessed as **Medium** and **Low** risks, primarily due to their assessed Likely likelihoods.

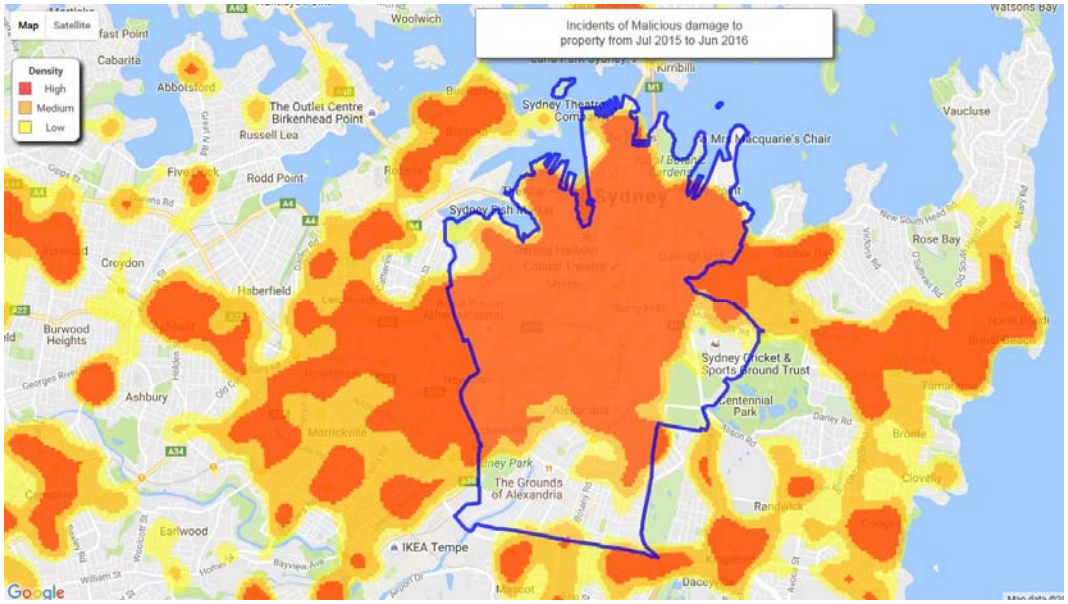
Crime Statistics

Malicious damage to property is the fourth most prevalent offence type to occur within the Sydney LGA. 753 of the 2,691 malicious damage to property offences occurred within an outdoor/public place setting.

Crime Hot Spots

The map below portrays the malicious damage to property hotspots for the entire City of Sydney LGA:

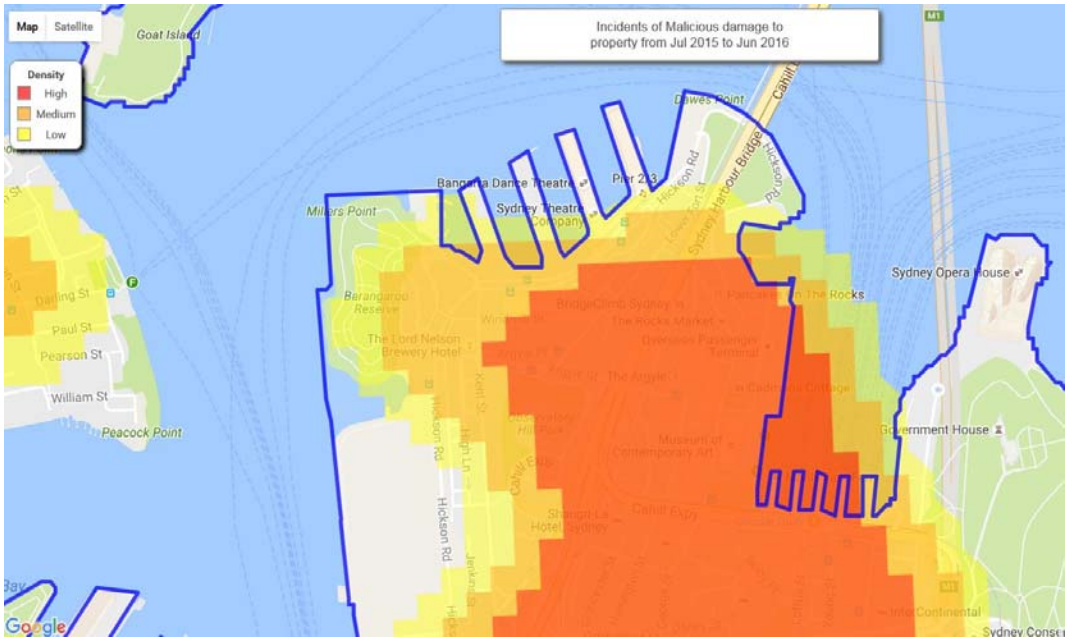
Figure 5 - Sydney LGA Malicious Damage Hot Spot



Source: BOCSAR

The map below portrays the malicious damage to property hotspots for the WBAP area:

Figure 6 - WBAP Area Malicious Damage Hotspot



Source: BOCSAR

As can be seen in the hot spot maps above, malicious damage to property offences are fairly prevalent within the Sydney LGA, but less prevalent within the WBAP area.

Risk Analysis

Malicious damage to property is the fourth most prevalent offence type to occur within the Sydney LGA. 753 of the 2,691 malicious damage to property offences occurred within an outdoor/public place setting.

Those most likely to commit malicious damage to property offences within the Sydney LGA are men aged 20-29. Malicious damage to property offences within the Sydney LGA are generally not alcohol related, with only 15.3% attributed with alcohol consumption. Malicious damage to property offences are most likely to occur within the Sydney LGA between the hours of 12-6am on a Sunday morning.

The number of malicious damage to property offences has decreased by 25.23% over the past five years, and 19.50% over the last three years, making it likely that the risks posed to the WBAP by this offence type will continue to decline.

8.3.8 Steal from Motor Vehicle Offences

Risk Rating

Steal from motor vehicles have been assessed as **Medium** risks, based on their Likely likelihood.

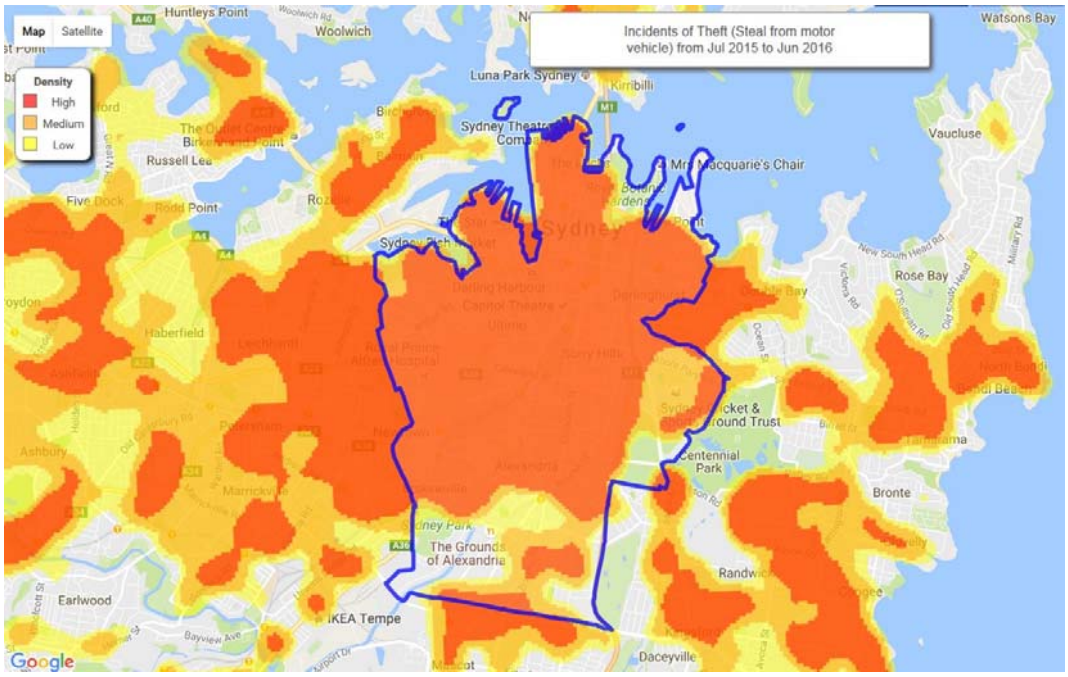
Crime Statistics

Steal from motor vehicles is the fifth most prevalent offence type to occur within the Sydney LGA, and the second most prevalent offence category within Outdoor/Public Place settings.

Crime Hot Spots

The map below portrays the steal from motor vehicle hotspots for the entire City of Sydney LGA:

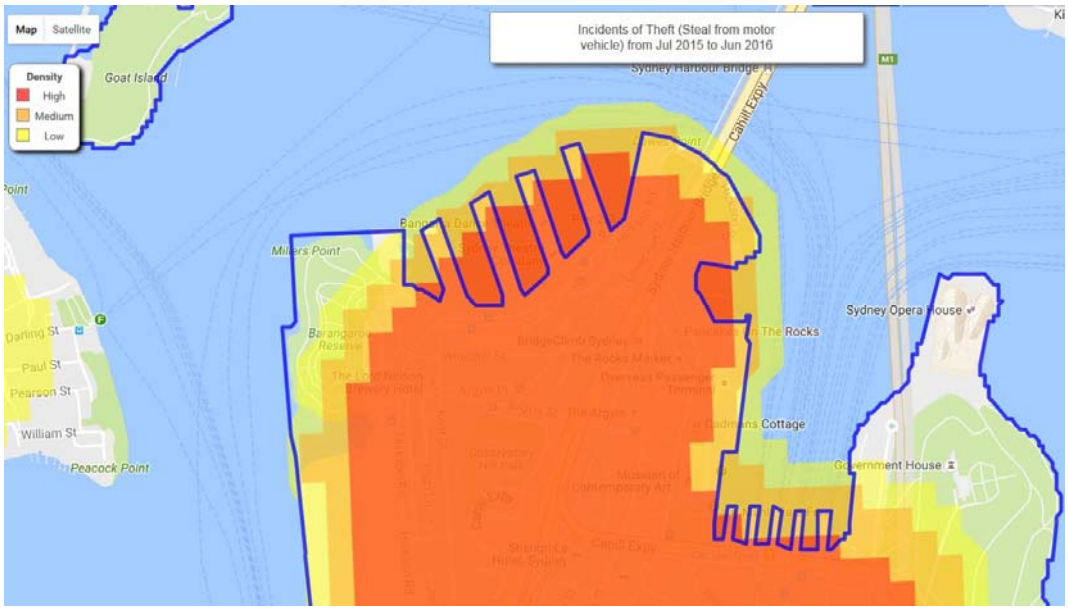
Figure 7 - Sydney LGA Steal from Motor Vehicle Hotspot



Source: BOCSAR

The map below portrays the steal from motor vehicle hotspots for the WBAP area:

Figure 8 - WBAP Area Steal from Motor Vehicle Hotspot



Source: BOCSAR

As can be seen in the hot spot maps above, steal from motor vehicle offences occur fairly evenly throughout the Sydney LGA, including the WBAP area.

Risk Analysis

Steal from motor vehicles is the fifth most prevalent offence type to occur within the Sydney LGA, and the second most prevalent offence category within

Outdoor/Public Place settings. Of the 1,686 steal from motor vehicle offences within the Sydney LGA during 2015, 1,028 were recorded within an Outdoor/Public Place setting.

Those most likely to steal from motor vehicles within the Sydney LGA are men aged 40+ and are most likely to occur between the hours of 12-6pm on a Sunday afternoon. Steal from motor vehicle offences are not alcohol related, with only 13 out of the 1,673 offences attributed to the consumption of alcohol.

The number of steal from motor vehicle offences has decreased by 37.85% over the last five years, and 28.29% over the last three years, making it likely that the risks posed to the WBAP by this offence type will continue to decrease.

8.3.9 Steal from Person Offences

Risk Rating

Steal from person offences have been assessed as **Low** risks, based on their Minimal consequences.

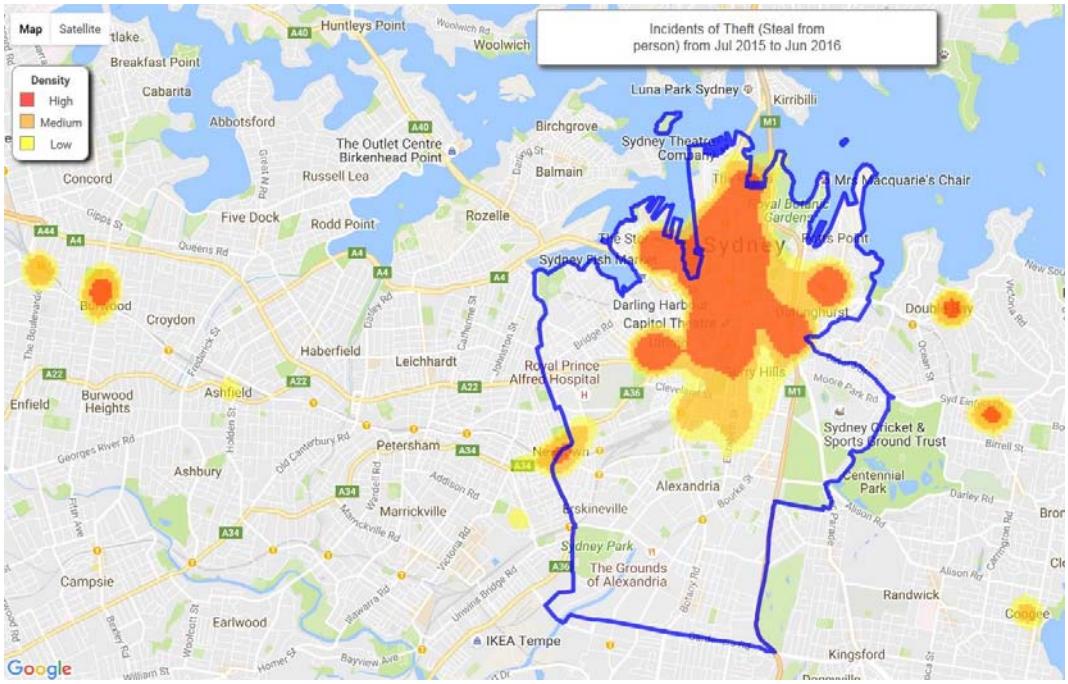
Crime Statistics

Steal from person is the sixth most prevalent offence type to occur within the Sydney LGA, and the fourth most prevalent offence category within Outdoor/Public Place settings.

Crime Hot Spots

The map below portrays the steal from person hotspots for the entire City of Sydney LGA:

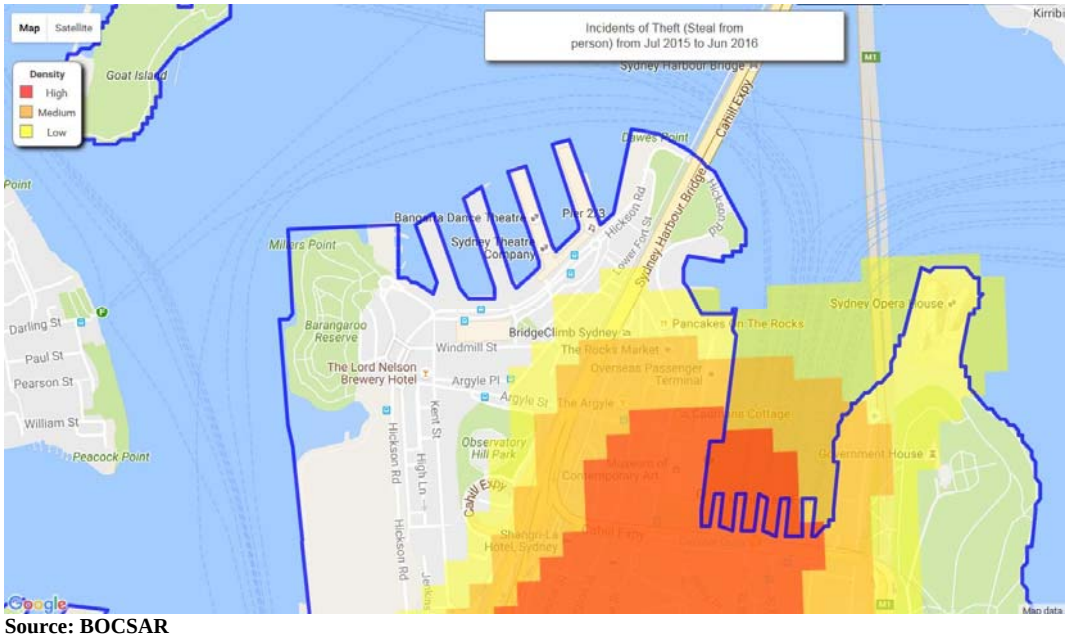
Figure 9 - Sydney LGA Steal from Person Hotspot



Source: BOCSAR

The map below portrays the steal from person hotspots for the WBAP area:

Figure 10 - WBAP Area Steal from Person Hotspot



Source: BOCSAR

As can be seen in the hot spot maps above, within the Sydney LGA, steal from person offences tend to occur within the CBD, Surrey Hills, Kings Cross, and Ultimo areas. Steal from person offences do not tend to occur within the WBAP area.

Risk Analysis

Steal from person is the sixth most prevalent offence type to occur within the Sydney LGA, and the fourth most prevalent offence category within Outdoor/Public Place settings. 453 of the 1,661 steal from person offences within the Sydney LGA during 2015 were recorded within an Outdoor/Public Place setting.

Those most likely to steal from people within the Sydney LGA are men aged 20-29, and are most likely to occur between the hours of 12-6am on a Sunday morning. Women aged 18-29 are most likely to be the victims of this offence. 8.1% of steal from person offences attributed to the consumption of alcohol.

The number of steal from person offences has decreased by 42.35% over the last five years, and 25.35% over the last three years, making it likely that the risks posed to the WBAP by this offence type will continue to decrease.

8.3.10 Harassment, Threatening Behaviour and Public Nuisance Offences

Risk Rating

Harassment, threatening behaviour and public nuisance has been assessed as **Medium** risks, primarily due to their assessed Likely and Almost Certain likelihood.

Crime Statistics

Harassment, threatening behaviour and public nuisance offences are the 10th most prevalent offence type to occur within the Sydney LGA.

Crime Hot Spots

Crime hot spots are not available for this offence category.

Risk Analysis

Premises type, victim, offender, alcohol related, and time of offence data for harassment, threatening behaviour and public nuisance offences is not recorded by BOCSAR.

The number of harassment, threatening behaviour and public nuisance offences has reduced by 3.49% over the past five years, and by 8.39% over the last three years within the Sydney LGA, making it likely that the risks posed to the WBAP by this offence type will stay the same or decline in the future.

8.4 Analysis of Terrorism Based Risks

8.4.1 Overview

Terrorism based security risks such as PBIED's, placed IED's, active shooters, knife attacks, siege/hostage scenarios, or chemical/biological/radiological (CBR) risks represent a **High** level of security risk to the WBAP. It should be noted that these terrorist type risks have been rated as Rare or Unlikely, and their **High** risk rating is due to their potential Catastrophic consequence rating.

The likelihood rating for these terrorist type activities has been based on the current National Terrorism Threat level, and the historical occurrence of these types of events taking place in Outdoor/Public Place settings within Australia and around the world. Historically, within Australia the main targets of terrorist attacks has been consulates, police stations, and locations linked with particular religious or cultural groups. Furthermore places of mass gathering, iconic locations, and symbols of government (Defence/Police/Political locations) represent attractive targets for terrorists.

8.4.2 Current Terrorism Threat Level

Australia's current National Terrorism Threat level (at the date of this report) is **Probable**.

The National Terrorism Threat level is a scale of five levels to provide advice about the likelihood of an act of terrorism occurring in Australia. The five levels are:

- **Certain** – A terrorist attack will soon occur or is underway;
- **Expected** - A terrorist attack is not expected;
- **Probable** – A terrorist attack is probable;

- **Possible** – A terrorist attack is possible; and
- **Not Expected** – A terrorist attack is not expected.

The National Terrorism Threat level guides national preparation and planning, and it also dictates the levels of precaution and vigilance to minimise the risk of a terrorist incident occurring. The Australian Government regularly reviews these alert levels.

The Australian National Terrorism Threat level has been rated as Probable since the new national terrorism threat advisory system was launched on 26 November 2015. This rating is based on credible intelligence which indicates that individuals or groups have developed both the intent and capability to conduct a terrorist attack in Australia.

The rating is not based on knowledge of a specific attack plan but rather a body of evidence that points to the increased likelihood of a terrorist attack in Australia.

8.4.3 Historical Terrorist Incidents - Australia

Over the last four years, 23 people have been convicted of terrorism offences in Australia. There has also been a number actual terrorist attacks within Australia over the years, with the most recent attack being the shooting and killing of a civilian NSW Police employee in Parramatta by Farhad Mohammad, in October 2015. Other notable Australian terrorist attacks include:

- The ‘Sydney Siege’, carried out in Martin Place on 15-16th December 2014 by Man Haron Monis;
- The stabbing of two police officers in Endeavour Hills, Victoria by Numan Haider, in September 2014;
- The East Melbourne Family Planning Clinic Attack (2001, VIC);
- Perth French Consulate Bombing (1995, WA);
- Turkish Consulate Bombing (1986, VIC);
- Melbourne Police Station Bombing (1986, VIC);
- Israeli Consulate Bombing (1982, NSW);
- Hakoah Club Bombing (1982, NSW);
- The Australian Nationalist Movement (ANM) Attacks (1980’s & 2004, WA);
- Sydney Turkish Consul General assassination (1980, NSW);
- Sydney Hilton Bombing (1978, NSW);
- Sydney Yugoslav General Trade and Tourist Agency Bombing (1972, NSW); and
- The Ustase Attacks (1970’s, Aus).

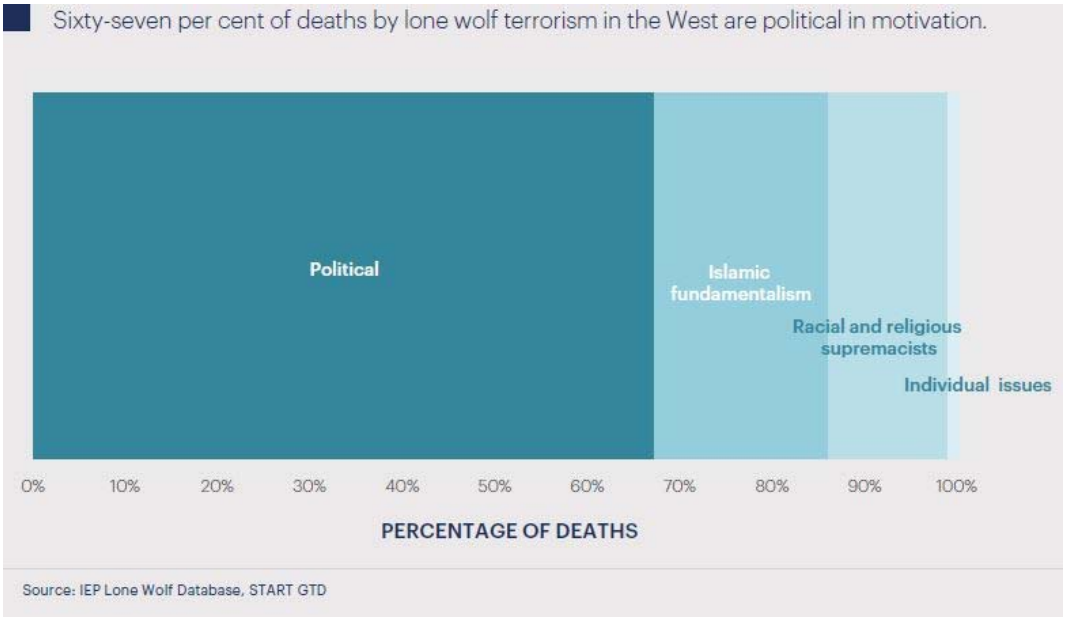
8.4.4 Terrorism Risk Analysis - General

It should be noted that over the last 15 years, only 4.4% of global terrorist attacks, and 2.6% of terrorist attack related deaths have occurred within western countries. Of these terrorist attack deaths within western countries, 91% of the deaths occurred from just 4 attacks – September 11, the Madrid Train Bombings, the Norwegian Massacre, and the London Bombings.

The main terrorist threat source to Australia comes from lone wolf terrorists. Lone wolf terrorists are individuals or a small number of individuals who commit an attack in support of a group, movement or ideology without material assistance or orders from a terrorist group.

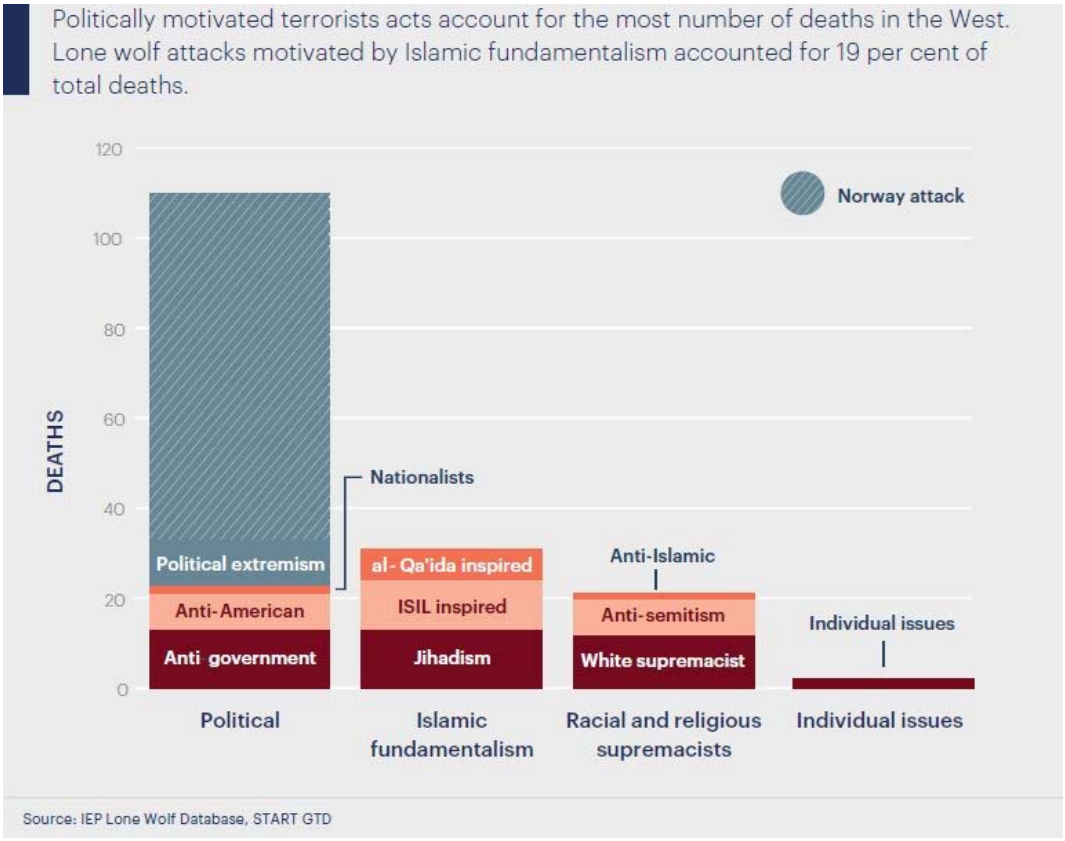
Close to 70% of all deaths in the West from terrorist attacks between 2006 and 2014 came from lone wolf attacks, as can be seen in the figure below. Lone wolf attacks in western countries are also not exclusively inspired by the calls for international jihad by groups such as Islamic State or Al–Qa'ida, as political attacks represent the largest category, with 67% of deaths by lone wolf attacks in the West. Despite Islamic Fundamentalism representing only about 19% of all terrorist attack related deaths in the west, it has been the main driving factor of terrorist attacks and plots within Australia over the last 5 years.

Figure 11 - Deaths by Lone Wolf Terrorists in Western Countries by Category, 2006-2014



Source: Lone Wolf Database, START GTD

Figure 12 - Number of Deaths by Lone Wolf Terrorists in Western Countries by Motivation, 2006-2014



Source: Lone Wolf Database, START GTD

8.4.5 Hostile Vehicle Attack

Overview

Hostile vehicle attacks are a high concern attack method as they are easy to carry out, often difficult to protect against, and require little planning and resources. They can also be highly effective, as evident in the 2016 Nice, France Attack.

WBAP Risk

Due to the layout of the WBAP, a hostile vehicle attack via a road vehicle is not considered a realistic security risk. There is limited, and indirect vehicle access to the main public realm areas, in particular the waterfront square. High approach speeds are also not achievable. A HVM attack via a marine vessel to deliberately damage infrastructure or to injure people is also considered to have a rare likelihood.

8.4.6 Vehicle Borne IED's

Overview

Vehicle Borne IED's are an especially catastrophic attack method, which often target places of mass gathering or critical, or symbolic infrastructure.

WBAP Risk

Due to the layout of the WBAP, a VBIED attack delivered via a road vehicle is not considered a realistic security risk, as there is limited vehicle access to the main public realm areas, in particular the waterfront square. The public realm areas and places of mass gathering are also sheltered on three sides by tall buildings, and the harbour on the other side. A VBIED delivered via a marine vessel is also regarded as rare likelihood.

It is also difficult to source the amount of chemical precursors required to make a VBIED, particularly to source them undetected.

A number of other event and performance locations within Sydney are also more desirable targets.

8.4.7 Person Borne/Placed IED's

Overview

Person borne and placed IED's are effective attack methods, which are difficult to protect against. Places of mass gathering, iconic and symbolic locations, and transport infrastructure are often targeted by this attack method.

WBAP Risk

PBIED's and placed IEDs do require a high degree of knowledge, skills, and resources to carry out. However, there is plenty of freely available information on how to carry out this attack method, and it is a commonly used method by terrorists. It is somewhat difficult to source the required chemicals and precursors to make PBIED's, particularly to source them undetected. However due the lower amount required, it is far more achievable than VBIED's.

As a place of mass gathering, the WBAP would be the type of location targeted by this attack method, however, a number of other event and performance locations within Sydney are considered more desirable targets (e.g. Opera House, SCG, the Olympic Stadium, Circular Quay, and Darling Harbour etc.).

8.4.8 Active Shooter

Overview

Active shooter is an effective attack method, which is difficult to protect against. Places of mass gathering, iconic and symbolic locations are often targeted by this attack method.

WBAP Risk

Active shooter attacks are easy to carry out, often difficult to protect against, and require little planning and resources. This attack method has been recently used to carry out a terrorist act within Sydney (2015 Parramatta Shooting at NSWPF headquarters).

As a place of mass gathering, the WBAP would be the type of location targeted by this attack method, however, a number of other event and performance locations within Sydney are considered more desirable targets (e.g. Opera House, SCG, the Olympic Stadium, Circular Quay, and Darling Harbour etc.).

8.4.9 Knife Attack

Overview

Knife attacks are an effective attack method, which is difficult to protect against. Places of mass gathering, iconic and symbolic locations, and transport infrastructure are often targeted by this attack method.

WBAP Risk

Knife attacks are easy to carry out, very difficult to protect against, and require little planning and resources. Global terrorist groups such as Islamic State have actively called for knife attacks to be carried out in western countries, including Australia. This attack method was recently used within Australia, with the stabbing of two police officers in Endeavour Hills, Victoria in September 2014. A number of planned knife attacks within Sydney have also been prevented.

As a place of mass gathering, the WBAP would be the type of location targeted by this attack method, however, a number of other event and performance locations within Sydney are considered more desirable targets (e.g. Opera House, SCG, the Olympic Stadium, Circular Quay, and Darling Harbour etc.).

9 Risk Evaluation

9.1 General

The purpose of security risk evaluation is to assist in making decisions, based on the outcomes of the risk analysis, about which security risks require treatment (risk tolerance), and the priority for the treatment implementation.

9.2 Tolerance of Security Risk

Decisions on the tolerability of the identified security risks have been based upon the As Low As Reasonably Practicable (ALARP) approach depicted in the Figure below. This approach recognises the concept of a gradient of tolerability but divides the gradient up into three broad bands based upon a:

- Broadly acceptable region, where risk reduction is not likely to be required as any benefits realised are likely to be outweighed by costs;
- Tolerable region (the ALARP region) where the risk is regarded as tolerable only if further risk reduction is impracticable (for example because of cost benefit considerations or an absence of a feasible solution); and
- Broadly unacceptable region where risk cannot be justified, except in extraordinary circumstances.

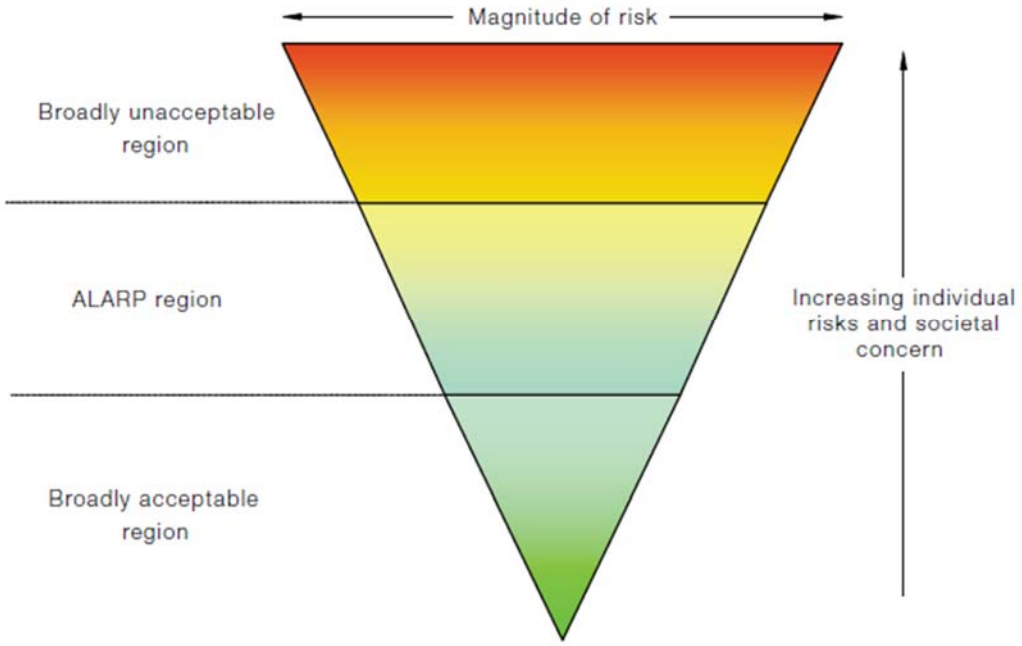


Figure 13 - ALARP Approach

Broadly Unacceptable Region:

Extreme risks are regarded as unacceptable, and require immediate action in order to reduce them as low as reasonably possible.

ALARP Region:

Tolerable risks (High and Medium) are required to be reduced as low as reasonably possible.

Broadly Acceptable Region:

Broadly Acceptable (Low) risks are broadly acceptable and only need to be managed through routine procedures.

9.3 Security Risk Evaluation

Each identified security risk has been evaluated, and ranked based on their tolerability, with the least tolerable, and therefore priority risks to be treated listed first.

Table 11 - Security Risk Evaluation

Security Risk	Security Risk Event	Evaluation of Existing Controls	Consequence	Likelihood	Security Risk Rating	Evaluation of Tolerability
Hostage / Siege	Within public realm	Inadequate	Catastrophic	Unlikely	**High**	**May be Tolerable**
Hostage / Siege	Within performance / function / event spaces	Inadequate	Catastrophic	Unlikely	**High**	**May be Tolerable**
Hostile Vehicle attack (car or boat)	Within public realm	Adequate	Catastrophic	Rare	**High**	**May be Tolerable**
Placed/Person Borne IED	Within waterfront square	N/A	Catastrophic	Unlikely	**High**	**May be Tolerable**
Placed/Person Borne IED	Within performance / function / event spaces	Inadequate	Catastrophic	Unlikely	**High**	**May be Tolerable**
Vehicle Borne IED (car or boat)	Within public realm	Adequate	Catastrophic	Rare	**High**	**May be Tolerable**
CBR attack	Within public realm	Inadequate	Catastrophic	Unlikely	**High**	**May be Tolerable**

Security Risk	Security Risk Event	Evaluation of Existing Controls	Consequence	Likelihood	Security Risk Rating	Evaluation of Tolerability
CBR attack	Within waterfront square	N/A	Catastrophic	Unlikely	**High**	**May be Tolerable**
CBR attack	Within performance / function / event spaces	Inadequate	Catastrophic	Unlikely	**High**	**May be Tolerable**
Knife attack	Within public realm	Inadequate	Catastrophic	Unlikely	**High**	**May be Tolerable**
Knife attack	Within waterfront square	N/A	Catastrophic	Unlikely	**High**	**May be Tolerable**
Knife attack	Within performance / function / event spaces	Inadequate	Catastrophic	Unlikely	**High**	**May be Tolerable**
Active shooter	Within public realm	Inadequate	Catastrophic	Rare	**High**	**May be Tolerable**
Active shooter	Within waterfront square	N/A	Catastrophic	Rare	**High**	**May be Tolerable**
Active shooter	Within performance / function / event spaces	Inadequate	Catastrophic	Rare	**High**	**May be Tolerable**
Assault	Assault of patrons within public realm	Inadequate	Minimal	Likely	**Medium**	**Tolerable**
Assault	Assault of patrons within waterfront square	N/A	Minimal	Likely	**Medium**	**Tolerable**
Assault	Indecent assault of patrons within public realm	Inadequate	Minor	Possible	**Medium**	**Tolerable**
Theft	Theft from café	Inadequate	Minimal	Likely	**Medium**	**Tolerable**
Theft	Theft from merchandise store	Inadequate	Minimal	Likely	**Medium**	**Tolerable**
Theft	Theft from store rooms	Inadequate	Minor	Likely	**Medium**	**Tolerable**

Security Risk	Security Risk Event	Evaluation of Existing Controls	Consequence	Likelihood	Security Risk Rating	Evaluation of Tolerability
Theft	Theft from box office/cloak room	Inadequate	Minor	Likely	**Medium**	**Tolerable**
Theft	Theft from bar store	Inadequate	Minor	Likely	**Medium**	**Tolerable**
Theft	Theft of vehicles	Inadequate	Minor	Likely	**Medium**	**Tolerable**
Theft	Theft from vehicles	Inadequate	Minor	Likely	**Medium**	**Tolerable**
Vandalism	Malicious damage/graffiti of WBAP buildings	Inadequate	Minor	Likely	**Medium**	**Tolerable**
Vandalism	Malicious damage/graffiti of public realm infrastructure & assets	Inadequate	Minor	Likely	**Medium**	**Tolerable**
Antisocial Behaviour	Harassment, threatening behaviour, public nuisance, offensive conduct within public realm	Inadequate	Minimal	Almost Certain	**Medium**	**Tolerable**
Antisocial Behaviour	Harassment, threatening behaviour, public nuisance, offensive conduct within WBAP buildings	Inadequate	Minimal	Likely	**Medium**	**Tolerable**
Antisocial Behaviour	Drug use and/or possession within public realm	Inadequate	Minimal	Almost Certain	**Medium**	**Tolerable**
Antisocial Behaviour	Intoxicated persons within public realm	Inadequate	Minimal	Almost Certain	**Medium**	**Tolerable**
Antisocial Behaviour	Intoxicated persons within Level 1 pier 2/3 bar	Inadequate	Minimal	Almost Certain	**Medium**	**Tolerable**
Antisocial Behaviour	Intoxicated persons within Bar at the end of the wharf	Inadequate	Minimal	Almost Certain	**Medium**	**Tolerable**

Security Risk	Security Risk Event	Evaluation of Existing Controls	Consequence	Likelihood	Security Risk Rating	Evaluation of Tolerability
Antisocial Behaviour	Intoxicated persons within commercial/function spaces	Inadequate	Minimal	Almost Certain	**Medium**	**Tolerable**
Trespass	Break & enter into WBAP buildings	Inadequate	Minimal	Likely	**Medium**	**Tolerable**
Trespass	Unauthorised access to back of house areas	Inadequate	Minimal	Likely	**Medium**	**Tolerable**
Trespass	Break & enter/unauthorised access into plant areas	Inadequate	Minor	Possible	**Medium**	**Tolerable**
Trespass	Unauthorised access to office areas	Inadequate	Minor	Possible	**Medium**	**Tolerable**
Murder / Attempted Murder	Within public realm	Inadequate	Major	Rare	**Medium**	**Tolerable**
Murder / Attempted Murder	Within WBAP buildings	Inadequate	Major	Rare	**Medium**	**Tolerable**
Arson	Deliberate act to damage facilities or to disrupt operations	Inadequate	Major	Rare	**Medium**	**Tolerable**
Arson	Deliberate act to damage public realm infrastructure or to disrupt operations	Inadequate	Major	Unlikely	**Medium**	**Tolerable**
Protest / Demonstration	Protest or demonstration by Issue Motivated Groups resulting in illegal occupation of the public realm, unwanted media exposure, interruption to operations, etc.	Inadequate	Moderate	Unlikely	**Medium**	**Tolerable**
Protest / Demonstration	Protest or demonstration by Issue Motivated Groups resulting in illegal occupation of the WBAP	Inadequate	Moderate	Unlikely	**Medium**	**Tolerable**

Security Risk	Security Risk Event	Evaluation of Existing Controls	Consequence	Likelihood	Security Risk Rating	Evaluation of Tolerability
	buildings, unwanted media exposure, interruption to operations, etc.					
Abduction / Kidnapping	From within public realm	Inadequate	Major	Rare	**Medium**	**Tolerable**
Abduction / Kidnapping	From within WBAP buildings	Inadequate	Major	Rare	**Medium**	**Tolerable**
Assault	Assault of patrons within Pier 2/3, Wharf 4/5 commercial/function spaces	Inadequate	Minimal	Unlikely	**Low**	**Broadly Acceptable**
Assault	Assault of patrons within bar at the end of the wharf	Inadequate	Minimal	Possible	**Low**	**Broadly Acceptable**
Assault	Assault of staff within public realm	Inadequate	Minimal	Possible	**Low**	**Broadly Acceptable**
Assault	Assault of staff within waterfront square	N/A	Minimal	Possible	**Low**	**Broadly Acceptable**
Assault	Assault of staff within Pier 2/3, Wharf 4/5 commercial/function spaces	Inadequate	Minimal	Unlikely	**Low**	**Broadly Acceptable**
Assault	Assault of staff at box office/reception desks/concierge	Inadequate	Minimal	Unlikely	**Low**	**Broadly Acceptable**
Assault	Assault of staff within bar at the end of the wharf	Inadequate	Minimal	Possible	**Low**	**Broadly Acceptable**
Assault	Assault of staff at Level 1 Pier 2/3 bar	Inadequate	Minimal	Possible	**Low**	**Broadly Acceptable**
Assault	Assault of patrons at Level 1 Pier 2/3 bar	Inadequate	Minimal	Possible	**Low**	**Broadly Acceptable**

Security Risk	Security Risk Event	Evaluation of Existing Controls	Consequence	Likelihood	Security Risk Rating	Evaluation of Tolerability
Assault	Indecent assault of patrons within WBAP buildings	Inadequate	Minor	Unlikely	**Low**	**Broadly Acceptable**
Assault	Indecent assault of staff within public realm	Inadequate	Minor	Unlikely	**Low**	**Broadly Acceptable**
Assault	Indecent assault of staff within WBAP buildings	Inadequate	Minor	Unlikely	**Low**	**Broadly Acceptable**
Theft	Theft from commercial/function spaces	Inadequate	Minimal	Possible	**Low**	**Broadly Acceptable**
Theft	Theft from cleaners store room	Inadequate	Minimal	Unlikely	**Low**	**Broadly Acceptable**
Theft	Theft from office areas	Inadequate	Minimal	Possible	**Low**	**Broadly Acceptable**
Theft	Theft from Level 1 pier 2/3 bar	Inadequate	Minimal	Possible	**Low**	**Broadly Acceptable**
Theft	Theft from bar at the end of the wharf	Inadequate	Minimal	Possible	**Low**	**Broadly Acceptable**
Robbery/ Steal from person	Robbery/steal from staff within public realm/waterfront square	Inadequate	Minimal	Possible	**Low**	**Broadly Acceptable**
Robbery/ Steal from person	Robbery/steal from patrons within public realm/waterfront square	Inadequate	Minimal	Possible	**Low**	**Broadly Acceptable**
Robbery/ Steal from person	Robbery/steal from staff within WBAP buildings	Inadequate	Minimal	Unlikely	**Low**	**Broadly Acceptable**
Robbery/ Steal from person	Robbery/steal from patrons within with in WBAP buildings	Inadequate	Minimal	Unlikely	**Low**	**Broadly Acceptable**

Security Risk	Security Risk Event	Evaluation of Existing Controls	Consequence	Likelihood	Security Risk Rating	Evaluation of Tolerability
Vandalism	Malicious damage/graffiti within WBAP buildings	Inadequate	Minimal	Unlikely	**Low**	**Broadly Acceptable**
Antisocial Behaviour	Drug use and/or possession within WBAP buildings	Inadequate	Minimal	Possible	**Low**	**Broadly Acceptable**
Antisocial Behaviour	Drug dealing within public realm	Inadequate	Minimal	Possible	**Low**	**Broadly Acceptable**
Antisocial Behaviour	Drug dealing within WBAP buildings	Inadequate	Minimal	Unlikely	**Low**	**Broadly Acceptable**
Trespass	Break & enter into commercial areas	Inadequate	Minimal	Possible	**Low**	**Broadly Acceptable**

9.4 Evaluation of Existing Controls

9.4.1 Overview

The existing security control measures for every identified security risk has been assessed. Of the 72 identified security risks, 64 have been assessed as having inadequate existing controls. The existing controls for two of the identified risks were assessed as adequate. The assessment of the existing control measures was not relevant for 6 identified security risks, therefore there was no assessment. Due to this inadequate assessment of existing controls, a number of new and/or additional treatment measures have been recommended.

9.4.2 Evaluation Outcome

Table 12 - Evaluation Outcome

		Evaluation of Existing Controls				
		Adequate	Opportunities for Improvement	Inadequate	No Assessment	Totals
Risk Priority	Extreme	0	0	0	0	0
	High	2	0	9	4	15
	Medium	0	0	30	1	31
	Low	0	0	25	1	26
	Totals	2	0	64	6	72

9.5 Risk Treatment Priorities

9.5.1 Risks to Treat

High and Medium are required to be reduced as low as reasonably possible and should be prioritised.

Low risks are broadly acceptable and only need to be managed through routine procedures.

9.5.2 Priority Risks

The assessed High risks should be prioritised, however as the High risks are all terrorist based risks that have been assessed as Rare or Unlikely, reasonable measures should only be implemented where practical.

10 Risk Treatment

10.1 Overview of Treatment Options

Broadly speaking, options for the treatment of security risk will involve one or a combination of the following treatment strategies:

- **Reduce:** control improvements or new controls (treatments) are introduced that are aimed at reducing the consequence or likelihood of the risk, e.g. to improve:
    - Deterrence of the threat;
    - Delay of an event;
    - Detection and investigation of the event;
    - Response to the event or its consequence;
    - Recovery from the event and its consequences; or
    - Prosecution of individuals or groups involved in perpetrating the event.
- **Avoid:** the likelihood of security risk is reduced or removed by ceasing the individual's, organisation's or community's activities that create an exposure (e.g. prevention of personal safety risk by not undertaking overseas travel to a specific location at that time);
- **Share:** The management of the security risk is 'shared' with a third party reducing the consequences of the risk (e.g. Police, insurance, outsourcing to a private Security Company). The sharing of risk is also commonly referred to the 'transfer' of risk to third parties. However, in reality only part of the responsibility for managing the risk can be transferred, some responsibility and all accountability for the risk remains with the first party; and
- **Tolerate, retain and monitor:** The risk is tolerable and retention of the risk is determined as a potential treatment strategy. Alternatively, the risk may be acknowledged as intolerable, but at the current time, capability or resources are unavailable, or treatment is not cost-effective. Therefore the only option may be to retain the risk and to continue to monitor it until circumstances change and action can be taken. After treatments have been implemented there will usually be some degree of residual risk. The decision will have to made as to whether this residual risk is tolerable and can be retained, or if further treatment is required.

10.2 Security Risk Treatments

Table 13 - Security Risk Treatments

Security Risk	Security Risk Event	Treatment Option	Recommended Treatment Measures
Assault	Assault of patrons within public realm	Reduce Likelihood	CCTV Help Points Improved Lighting On-site security guards Security signage
Assault	Assault of patrons within waterfront square	Reduce Likelihood	CCTV Help Points Improved Lighting On-site security guards Security signage
Assault	Assault of patrons within Pier 2/3, Wharf 4/5 commercial/function spaces	Reduce Likelihood	CCTV EACS Duress alarms On-site security guards
Assault	Assault of patrons within bar at the end of the wharf	Reduce Likelihood	CCTV EACS Duress alarms On-site security guards
Assault	Assault of staff within public realm	Reduce Likelihood	CCTV Help Points Improved Lighting On-site security guards Security signage
Assault	Assault of staff within waterfront square	Reduce Likelihood	CCTV Help Points Improved Lighting On-site security guards Security signage
Assault	Assault of staff within Pier 2/3, Wharf 4/5 commercial/function spaces	Reduce Likelihood	CCTV EACS Duress alarms On-site security guards
Assault	Assault of staff at box office/reception desks/concierge	Reduce Likelihood	CCTV EACS Duress alarms On-site security guards
Assault	Assault of staff within bar at the end of the wharf	Reduce Likelihood	CCTV EACS Duress alarms On-site security guards
Assault	Assault of staff at Level 1 Pier 2/3 bar	Reduce Likelihood	CCTV EACS Duress alarms On-site security guards
Assault	Assault of patrons at Level 1 Pier 2/3 bar	Reduce Likelihood	CCTV EACS Duress alarms On-site security guards
Assault	Indecent assault of patrons within public realm	Reduce Likelihood	CCTV Help Points Improved Lighting

Security Risk	Security Risk Event	Treatment Option	Recommended Treatment Measures
			On-site security guards Security signage
Assault	Indecent assault of patrons within WBAP buildings	Reduce Likelihood	CCTV EACS Duress alarms On-site security guards
Assault	Indecent assault of staff within public realm	Reduce Likelihood	CCTV Help Points Improved Lighting On-site security guards Security signage
Assault	Indecent assault of staff within WBAP buildings	Reduce Likelihood	CCTV EACS Duress alarms On-site security guards
Theft	Theft from café	Reduce Likelihood	CCTV EACS IAS On-site security guards Building perimeter physical security measures Room physical security measures
Theft	Theft from commercial/function spaces	Reduce Likelihood	CCTV EACS IAS On-site security guards Building perimeter physical security measures Room physical security measures
Theft	Theft from cleaners store room	Reduce Likelihood	CCTV EACS IAS On-site security guards Building perimeter physical security measures Room physical security measures
Theft	Theft from merchandise store	Reduce Likelihood	CCTV EACS IAS On-site security guards Building perimeter physical security measures Room physical security measures
Theft	Theft from store rooms	Reduce Likelihood	CCTV EACS IAS On-site security guards Building perimeter physical security measures Room physical security measures
Theft	Theft from office areas	Reduce Likelihood	CCTV EACS IAS On-site security guards Building perimeter physical security measures Room physical security measures
Theft	Theft from box office/cloak room	Reduce Likelihood	CCTV EACS IAS On-site security guards

Security Risk	Security Risk Event	Treatment Option	Recommended Treatment Measures
			Building perimeter physical security measures Room physical security measures
Theft	Theft from bar store	Reduce Likelihood	CCTV EACS IAS On-site security guards Building perimeter physical security measures Room physical security measures
Theft	Theft from Level 1 pier 2/3 bar	Reduce Likelihood	CCTV EACS IAS On-site security guards Building perimeter physical security measures Room physical security measures
Theft	Theft from bar at the end of the wharf	Reduce Likelihood	CCTV EACS IAS On-site security guards Building perimeter physical security measures Room physical security measures
Theft	Theft of vehicles	Reduce Likelihood	CCTV Security signage Improved lighting On-site security guards
Theft	Theft from vehicles	Reduce Likelihood	CCTV Security signage Improved lighting On-site security guards
Robbery/ Steal from person	Robbery/steal from staff within public realm/waterfront square	Reduce Likelihood	CCTV Help point Security signage Improved lighting On-site security guards
Robbery/ Steal from person	Robbery/steal from patrons within public realm/waterfront square	Reduce Likelihood	CCTV Help point Security signage Improved lighting On-site security guards
Robbery/ Steal from person	Robbery/steal from staff within WBAP buildings	Reduce Likelihood	CCTV EACS IAS On-site security guards Building perimeter physical security measures Room physical security measures Duress alarms
Robbery/ Steal from person	Robbery/steal from patrons within with in WBAP buildings	Reduce Likelihood	CCTV EACS IAS On-site security guards Building perimeter physical security measures Room physical security measures Duress alarms
Vandalism	Malicious damage/graffiti of WBAP buildings	Reduce Likelihood	CCTV Security signage Improved lighting On-site security guards

Security Risk	Security Risk Event	Treatment Option	Recommended Treatment Measures
Vandalism	Malicious damage/graffiti of public realm infrastructure & assets	Reduce Likelihood	CCTV Security signage Improved lighting On-site security guards
Vandalism	Malicious damage/graffiti within WBAP buildings	Reduce Likelihood	CCTV EACS IAS On-site security guards Building perimeter physical security measures Room physical security measures
Antisocial Behaviour	Harassment, threatening behaviour, public nuisance, offensive conduct within public realm	Reduce Likelihood	CCTV Help point Security signage Improved lighting On-site security guards
Antisocial Behaviour	Harassment, threatening behaviour, public nuisance, offensive conduct within WBAP buildings	Reduce Likelihood	CCTV EACS Duress alarms On-site security guards Building perimeter physical security measures Room physical security measures
Antisocial Behaviour	Drug use and/or possession within public realm	Reduce Likelihood	CCTV Help point Security signage Improved lighting On-site security guards
Antisocial Behaviour	Drug use and/or possession within WBAP buildings	Reduce Likelihood	CCTV On-site security guards
Antisocial Behaviour	Drug dealing within public realm	Reduce Likelihood	CCTV Help point Security signage Improved lighting On-site security guards
Antisocial Behaviour	Drug dealing within WBAP buildings	Reduce Likelihood	CCTV On-site security guards
Antisocial Behaviour	Intoxicated persons within public realm	Reduce Likelihood	CCTV Security signage Improved lighting On-site security guards Help points RSA
Antisocial Behaviour	Intoxicated persons within Level 1 pier 2/3 bar	Reduce Likelihood	CCTV On-site security guards RSA
Antisocial Behaviour	Intoxicated persons within Bar at the end of the wharf	Reduce Likelihood	CCTV On-site security guards RSA
Antisocial Behaviour	Intoxicated persons within commercial/function spaces	Reduce Likelihood	CCTV On-site security guards RSA
Trespass	Break & enter into WBAP buildings	Reduce Likelihood	CCTV EACS IAS On-site security guards Building perimeter physical security measures

Security Risk	Security Risk Event	Treatment Option	Recommended Treatment Measures
Trespass	Unauthorised access to back of house areas	Reduce Likelihood	CCTV EACS IAS On-site security guards Building perimeter physical security measures Room physical security measures
Trespass	Break & enter/unauthorised access into plant areas	Reduce Likelihood	CCTV EACS on building perimeter IAS On-site security guards Building perimeter physical security measures Room physical security measures
Trespass	Break & enter into commercial areas	Reduce Likelihood	CCTV EACS on building perimeter IAS On-site security guards Building perimeter physical security measures Room physical security measures
Trespass	Unauthorised access to office areas	Reduce Likelihood	CCTV EACS IAS On-site security guards Building perimeter physical security measures Room physical security measures
Murder / Attempted Murder	Within public realm	Reduce Consequence	CCTV Help point Security signage Improved lighting On-site security guards
Murder / Attempted Murder	Within WBAP buildings	Reduce Consequence	CCTV EACS IAS On-site security guards Building perimeter physical security measures Room physical security measures
Arson	Deliberate act to damage facilities or to disrupt operations	Reduce Consequence	CCTV EACS IAS On-site security guards Building perimeter physical security measures Room physical security measures Compliant fire detection and suppression strategy Operational response
Arson	Deliberate act to damage public realm infrastructure or to disrupt operations	Reduce Consequence	CCTV Help point Security signage Improved lighting On-site security guards Compliant fire detection and suppression strategy Operational response
Protest / Demonstration	Protest or demonstration by Issue Motivated Groups resulting in illegal occupation of the public realm, unwanted media	Reduce Consequence	CCTV Help point Security signage Improved lighting On-site security guards Operational response

Security Risk	Security Risk Event	Treatment Option	Recommended Treatment Measures
	exposure, interruption to operations, etc.		
Protest / Demonstration	Protest or demonstration by Issue Motivated Groups resulting in illegal occupation of the WBAP buildings, unwanted media exposure, interruption to operations, etc.	Reduce Consequence	CCTV Help point Security signage Improved lighting On-site security guards
Abduction/Kid napping	From within public realm	Reduce Likelihood	CCTV Help point Security signage Improved lighting On-site security guards
Abduction/Kid napping	From within WBAP buildings	Reduce Likelihood	CCTV EACS IAS On-site security guards Building perimeter physical security measures Room physical security measures
Hostage / Siege	Within public realm	Reduce Likelihood	CCTV Help point Security signage Improved lighting On-site security guards Operational response
Hostage / Siege	Within performance / function / event spaces	Reduce Likelihood	CCTV EACS Duress alarms On-site security guards Operational response Building perimeter physical security measures Room physical security measures
Hostile Vehicle attack	Within public realm	Reduce Consequence	CCTV Help point On-site security guards Operational response Precinct physical security measures (bollards, roller shutters etc.)
Placed/Person Borne IED	Within waterfront square	Reduce Likelihood	CCTV Help point On-site security guards Operational response Improved lighting
Placed/Person Borne IED	Within performance / function / event spaces	Reduce Likelihood	CCTV EACS Duress alarms On-site security guards Operational response Building perimeter physical security measures Room physical security measures
Vehicle Borne IED	Within public realm	Reduce Consequence	CCTV Help point Security signage Improved lighting On-site security guards

Security Risk	Security Risk Event	Treatment Option	Recommended Treatment Measures
			Operational response Precinct physical security measures (bollards, roller shutters etc.)
Knife attack	Within public realm	Reduce Likelihood	CCTV Help point Improved lighting On-site security guards Operational response
Knife attack	Within waterfront square	Reduce Likelihood	CCTV Help point Improved lighting On-site security guards Operational response
Knife attack	Within performance / function / event spaces	Reduce Likelihood	CCTV EACS Duress alarms On-site security guards Operational response Building perimeter physical security measures Room physical security measures
Active shooter	Within public realm	Reduce Likelihood	CCTV Help point Security signage Improved lighting On-site security guards Operational response
Active shooter	Within waterfront square	Reduce Likelihood	CCTV Help point Security signage Improved lighting On-site security guards Operational response
Active shooter	Within performance / function / event spaces	Reduce Likelihood	CCTV EACS Duress alarms On-site security guards Operational response Building perimeter physical security measures Room physical security measures
CBR attack	Within public realm	Tolerate	CCTV Help point Security signage Improved lighting On-site security guards Operational response
CBR attack	Within waterfront square	Tolerate	CCTV Help point Security signage Improved lighting On-site security guards Operational response
CBR attack	Within performance / function / event spaces	Tolerate	CCTV EACS Duress alarms On-site security guards Operational response

Security Risk	Security Risk Event	Treatment Option	Recommended Treatment Measures
			Building perimeter physical security measures Room physical security measures

11 Recommended Treatment Measures

11.1 General

The recommendations contained within this section of the report are based on the security risk treatment and mitigation measures contained within Section 0 and are based on Australian Security Standards, current security theories and reasonable industry practices.

These recommendations will help guide the security designs to be developed during the design phases of the project.

11.2 Design Measures

11.2.1 CPTED

It is recommended that the design and layout of the WBAP public realm, and waterfront square help facilitate crime prevention through environmental design (CPTED) aspects as far as practical. A review of the architectural designs from a CPTED perspective is recommended.

The designs should strive to achieve the following:

- Clutter free and minimalist design with plenty of glazing to ensure good natural surveillance, and minimise areas of possible concealment of people, actions or packages;
- Good lighting levels throughout the WBAP;
- Clear, open spaces;
- Clear, well defined footpaths and walkways;
- Security and way-finding signage throughout WBAP;
- Place making;
- Any vegetation within and immediately around the WBAP should be well maintained, and limited to either low height ground cover, or tall vegetation with clear trunks and high foliage that maintains clear sightlines; and
- Mixed use activation of the WBAP, in order to draw people to the area and prolong the time they spend in the area.

11.2.2 Defence in Depth (DiD)

It is recommended that the WBAP designs look to incorporate a defence in depth strategy. The underlying purpose of physical security is to delay an intruder for a sufficient amount of time until an appropriate response group has arrived to apprehend the offender. This delay can best be achieved through a series of barriers instead of a single strong barrier. The Defence in Depth security principle

imposes a succession of barriers, which require access, between the public and the asset.
It is recommended that the Defence in Depth strategy be used in conjunction with the Deter, Detect, Delay, and Respond security principle detailed below.

11.2.3 Deter, Detect, Delay, and Respond (D³R)

The D³R principle aims to deter an unauthorised intrusion from occurring at a particular location, detect the unauthorised intrusion as quickly as possible, and delay the intruder from reaching the desired asset for long enough for a suitable response force to arrive and apprehend the intruder before they reach or escape with the asset.

11.3 Electronic Security Measures

11.3.1 Monitoring Location

It is recommended that a central monitoring centre/location be provided to monitor, control, and administer the electronic security systems deployed throughout the WBAP (and other Arts facilities managed by Arts NSW, as required). The central monitoring location would provide operational command and control of the WBAP's security strategy day-to-day, and during events. This security monitoring centre should include functioning during normal and crisis modes as the primary operations centre. The security monitoring centre should coordinate with the Precinct Manager, in order to ensure the smooth, safe and secure operation of the WBAP. It is recommended that the security monitoring centre be located within the WBAP, but may be outsourced to a third party provider (a decision which is yet to be determined by INSW and Arts NSW).

11.3.2 CCTV

It is recommended that the base building closed circuit television (CCTV) system be expanded at WBAP to provide increased deterrence, surveillance and incidence capturing capabilities. Expansion to the CCTV system in line with the recommendations below will help treat the identified security risks as low as reasonably practicable. In addition to helping reduce the identified security risks, the CCTV system will also assist with the day-to-day security operations at the WBAP.

It is recommended that CCTV be provided to the following locations:

- General coverage throughout the WBAP;
- WBAP pedestrian entry/exit points;
- Roller shutters and boom gates;
- Building entry/exit points;
- Water based entry/exit points within the WBAP;
- Waterfront square and steps;

- Cafes, restaurants, bars, and function areas;
- Cash handling areas;
- High value item store entries;
- Box office and ticketing areas;
- Receptions;
- Foyers and lobbies;
- Lifts and stairs; and
- Key corridors.

11.3.3 Electronic Access Control System

It is recommended that the existing electronic access control system (EACS) be expanded at the WBAP to better electronically control access to restricted areas, and to provide an improved audit ability. Expansion of the EAC system in line with the recommendations below will help treat the identified security risks to as low as reasonably practicable. In addition to helping reduce the identified security risks, the EAC system will also assist with the day-to-day security operations at the WBAP.

Based on the identified security risks, it is recommended that EACS be provided/expanded to the following areas as a minimum:

Perimeter Doors

It is recommended that key perimeter doors have electronic access control in order to control and audit access into the buildings.

Front of House to Back of House Doors

It is recommended that doors leading from front of house to back of house areas have electronic access control.

Key Office Areas

Key offices and back of house rooms are recommended to have access control in order to control access to these areas, and to provide an audit function.

Fire Stairs

It is recommended that all fire stair doors not currently provided with EACS be upgraded so that each has a fail-safe electromechanical mortice lock. Fire stair doors are recommended to have free handle egress into the stairwell, and a fixed handle on the stairwell side of the door.

Each fire stair door should also be provided with local annunciation whenever there is a door held open.

In order to ensure BCA compliance with re-entry from fire-isolated exit requirements, it is recommended that an emergency break glass button and intercom is provided on every fourth floor.

The above recommendations will restrict inter-floor stairwell access to only those doors provided with access card readers, and will also prevent unauthorised access to floors via the stairwell.

Communications Room

Communications rooms are recommended to be provided with electronic access control in order to control access to critical building communications systems and to provide a record of access.

Roller Shutters/Boom Gates/Retractable Bollards

It is recommended that access control be provided to any roller shutters, boom gates, and retractable bollards in order to control and audit vehicle traffic into and out of the WBAP.

11.3.4 Intruder and Duress Alarm System

It is recommended that the existing intruder alarm system at the WBAP be expanded to monitor the integrity of the additional nominated areas. It is recommended that additional duress alarm devices be provided at the WBAP to allow staff to call for help/raise an alarm during emergency situations. Expansion of the intruder alarm system and duress alarm devices in line with the recommendations below will help treat the identified security risks as low as reasonably practicable. In addition to helping reduce the identified security risks, the intruder and duress alarm system will also assist with the day-to-day security operations at the WBAP.

Based on the identified security risks, it is recommended that intruder alarm devices be provided to the following areas as a minimum:

- Provide reed switch monitoring to:
    - All doors with electronic access control;
    - All perimeter doors;
    - Fire stairs doors;
    - Communications rooms;
    - Communications riser doors; and
    - Plant room doors.
- Provide PIR detectors to monitor:
    - Ground floor foyers and entries. IAS system to be integrated with the EAC system so that the PIR detectors are disabled by the successful badge of an authorised card on the external card reader.

Based on the identified security risks, it is recommended that duress alarm devices be provided to the following areas as a minimum:

- Reception desks;
- Bars;
- Box office/cloak room; and
- Accessible toilets.

An emergency help point system is also recommended to be provided within the public realm to allow patrons to call for assistance in emergency situations.

11.3.5 Intercom System

Based on the identified security risks, it is recommended that intercoms be provided to the following locations:

- Master intercom:
    - Monitoring location.
- Door station intercoms:
    - Fire stair doors on every fourth floor (i.e. Level 2), in line with BCA requirements;
    - Boom gate locations; and
    - Key building entries.

11.4 Physical Security Measures

It is recommended that increased physical security measures be provided at WBAP to help control access to assets, and restricted areas. Provision of physical security measures in line with the recommendations below will help treat the identified security risks as low as reasonably practicable. In addition to helping reduce the identified security risks, the physical security measures will also assist with the day-to-day security operations at WBAP.

Based on the identified security risks, it is recommended that the following physical security measures be provided where practical:

- It is recommended that strike shields be provided to the unsecure side of all outward opening perimeter doors;
- Provide high security SCEC endorsed mechanical keying systems on communications riser doors, switch room doors, any other key plant/services doors, and key store room doors. SCEC endorsed mechanical keying systems provide a restriction on unauthorised duplication of keys;
- It is recommended that security signage be provided at the main WBAP entry locations, key building entries, and throughout the public realm;

- It is recommended that the existing roller doors be replaced to ensure an adequate perimeter barrier is provided;
- It is recommended that the existing bollards be reviewed to ensure that they provide an appropriate function. Retractable bollards are proposed where vehicle access is required, in lieu of existing removable bollards. It is recommended that architectural vehicle mitigation measures be considered as well in lieu of bollards; and
- It is recommended that perimeter doors have an appropriate construction in order to provide appropriate protection against forced entry. Solid core doors with steel frames should be provided where possible.

11.5 Electronic Key Management System

It is recommended that an electronic key management system is provided to manage access to the mechanical keys used at WBAP, to provide an audit function of who has accessed specific keys, and to provide an alert function if keys are not returned.

11.6 Security Management Measures

It is recommended that the existing security management measures at WBAP be updated in line with the recommendations below to help treat the identified security risks as low as reasonably practicable.

Based on the identified security risks, it is recommended that the following security management measures be incorporated as a minimum:

- Continuously monitor the security risks and the effectiveness of security treatment measures through post event analysis and reporting;
- Periodic reviews of the security risks should be performed annually as a minimum, or when any of the follow occur:
    - Significant structural or layout changes made to the site or neighbouring premises;
    - Change of tenant at the site;
    - Significant changes to critical assets occur (e.g. new types of equipment purchased, changes in the confidential nature of information being used/stored, departure of staff with knowledge of access to potential vulnerabilities);
    - Significant changes occur in the local security environment (e.g. increase in offences locally);
    - The national security threat changes significantly (e.g. the National Terrorism Threat levels etc.);
    - Management responsibilities change significantly (e.g. appointment of a new senior manager/director);

  - New contractors/suppliers are appointed;
  - Availability and utility of security related technology changes;
  - There are significant changes in the nature of security risk within similar industries, markets, etc.;
  - Mergers/amalgamation/privatisation are occurring; and
  - Prior to any major event.

- The development and implementation of security management plans, policies and procedures. These policies and procedures should take into account changes in the National Terrorism Threat levels, and include procedures to communicate and respond to any changes in the alert levels;
- WBAP should regularly liaise with NSW Police, and NSW Counter-Terrorism Unit, as part of their continuous monitoring of security risks; and
- The development and implementation of emergency management plans, policies and procedures. These policies and procedures should also take into account changes in the National Terrorism Threat levels. These policies and procedures should also take into account other emergency situations that may affect operations such as fire and arson, major accidents, and natural disasters. These policies and plans should define how to minimise the risk of these events occurring through preventative measures and how to minimise their impact by appropriate response and business continuity measures (training, detection and suppression systems, evacuation procedures etc.).

11.7 Operational Security Measures

It is recommended that an on-site security presence be provided at WBAP on a 24/7 basis.

Security officers provide physical security presence throughout the WBAP, and are an important part of providing a deterrence effect to opportunistic crime. Security officers should irregularly patrol the WBAP, especially at night, and check doors are closed and locked, and windows are secured after hours.

Contract security officers are recommended to be stationed at WBAP at all times, with increased staffing for events. It is recommended that two security officers are stationed on site, with one providing a roaming guard service and the other monitoring security feeds on the CCTV system, electronic access control system, and other dedicated security systems.

Security officers should be responsible for responding to alarms, duress, and emergency calls, investigating as required to determine the cause of such events.

During events, this staffing level should be increased as required, with extra costs associated being passed on to the event.

Security officers should be uniformed to be clearly identifiable and visible in the WBAP.

12 Monitor and Review

12.1 General

The security risk environment is not constant. Organisations, communities and individuals are also in continual flux, sometimes discretely, often dramatically over short periods of time. Monitoring of risk provides the capability to respond effectively to changing environments. Therefore the entire security risk management process should be constantly monitored and regularly reviewed to ensure it remains current, efficient and effective.

The monitor and review step of the security risk management process has the objectives of achieving improved:

- Understanding, through:
    - Continuing awareness of changing contexts;
    - Continuing awareness of changing demands;
    - Learning from experience; and
    - Learning from others.
- Performance, through:
    - Managing stakeholder expectations;
    - Measurement/review of effectiveness of process elements;
    - Measurement/review of effectiveness of management of risks;
    - Identifying and implementing improvements; and
    - Enhancing integration with interdependencies.
- Assurance, through ensuring and confirming compliance with:
    - Strategic requirements;
    - Policy requirements;
    - Operational requirements; and
    - Regulatory requirements.

The concept of ‘monitor and review’ is based around the need to:

- Continuously examine the external and internal environments and reconsider the context and its effect on security risk management;
- Redevelop the analytical outputs of the security risk management process to reflect the changing context;
- Assess the efficiency and effectiveness of treatment plans in mitigating the risks identified;

- Re-evaluate the appropriateness of treatment activities to manage a dynamically changing risk environment;
- Measure the effectiveness and success of communications and consultation activities undertaken;
- Ensure that timely and adequate improvements are implemented;
- Continuously examine the conduct of the security risk management process and to adjust it to meet changing organisational needs and capability;
- Ensure appropriate governance through reporting to appropriate authorities, regulators, boards, stakeholders, management and staff as required; and
- Focus on both conformance and performance measurement.

12.2 Monitoring and Review Practices

Broadly speaking, there are four levels of monitoring practices that should be routinely observed:

- **Continuous monitoring**: that is undertaken on a frequent or ongoing basis, and involves routine checking by the process operators of changes in risk level, control breakdowns, incident occurrence, or established indicators of these (e.g. alarm monitoring). The aim is to ensure that implemented treatments and controls remain effective and that new risks are not being created. This process will also provide input into maintaining the currency of any security risk registers that have been developed;
- **Line management reviews**: periodic reviews of processes, policies, practices and systems, their risks and treatments. These reviews are often targeted at specific higher or changing risk issues (including assurance activities such as control self-assessments, etc.). The aim is to ensure that treatment and control strategies continue to be relevant, efficient and effective;
- **Centralised reviews**: by internal or external audit capability (e.g. security risk audits by a security consultant, NSW Police Force Counter Terrorism and Special Tactics Command, ASIO etc.). The aim is usually to ensure compliance with internal and externally mandated requirements so these reviews are highly selective in their focus. Reviews such as simulation exercises and penetration testing also provide awareness and training opportunities beyond the monitoring objectives; and
- **Scanning**: reviewing the internal and external environments for changing or emerging risk. The aim is to provide an early appreciation of emerging issues to allow sufficient time to act upon them. Although virtually essential at a strategic level, it should be adopted as a monitoring practice at all levels of the NRT organisation.

12.3 Triggering Monitoring and Review Processes

The Operator should ensure that a review of security risk is undertaken when:

- The national security threat changes significantly (e.g. the National Terrorism Threat Level etc.);
- There is a change in project phase (e.g. prior to changing from construction and commissioning phases to operation phase of the redevelopment);
- Significant structural or layout changes are made to the WBAP, or neighbouring premises;
- Significant changes to critical assets occur (e.g. new types of equipment purchased, changes in the confidential nature of information being used/stored, departure of staff with knowledge of access to potential vulnerabilities);
- Significant changes occur in the local security environment (e.g. increase in offences locally, at the WBAP);
- Significant changes occur in the external environment surrounding the WBAP and infrastructure (e.g. major changes to the type/nature of neighbouring premises);
- Management responsibilities change significantly (e.g. appointment of a new CEO);
- New contractors/suppliers are appointed;
- New tenants are appointed;
- Availability and utility of security related technology changes;
- There are significant changes in the nature of security risk within similar industries, markets, etc.;
- Mergers/amalgamation/privatisation are occurring; and
- Significant new events are provided at the WBAP.

Continual monitoring and review of the following aspects should be occurring at all stages of security risk assessment:

- The changing strategic, organisational and security risk contexts for changes that may impact upon the nature or level of risk to the individual, organisation or individual;
- The incidence, nature, types and impacts of security risk;
- The changing acceptability or tolerance of risk by the individual, organisation, community, or by their stakeholders;
- The effectiveness of security risk controls; and

- The effectiveness of security awareness programs and other communications initiatives.

12.4 Post Event Analysis and Reporting

Following any security risk-related event, a post-event analysis should be conducted to:

- Ensure that the incident and its aftermath were appropriately managed;
- Identify any learning's from the response to, and recovery from, the event and ensure that they are captured and used in subsequent improvement activities;
- Review to what extent the risk profile may have changed;
- Determine the effectiveness of the current control framework and existing treatment strategies and determine any additional treatment improvements that need to be made;
- Investigate and identify, where relevant, the perpetrators of the event and pursue them via administrative, civil or criminal process; and
- To communicate an improved understanding of security risk and its management to staff, and stakeholders, where appropriate.

Appendix A Standards and Guidelines

The following sections contain a list of the International and Australian standards, guidelines and handbooks that are relevant to this security risk assessment, and its recommended treatment measures. The documents below are recommended to be referred to where required.

- ISO 31000:2009: International Standard for Risk Management;
- HB 167:2006: Security Risk Management Handbook;
- HB 327:2010: Communicating and Consulting About Risk;
- AS 4806: Closed Circuit Television (Parts 1 – 4);
- AS 2201: Intruder Alarm Systems (Parts 1 – 4);
- AS 4421: Guards and Patrols; and
- National Guidelines for the Protection of Places of Mass Gathering.