

Prepared for  
UrbanGrowth NSW Development Corporation

---

2nd April 2019

# BAYS PRECINCT WEST EAST

**THE NEW SYDNEY FISH MARKET**

**SECURITY RISK  
ASSESSMENT REPORT**

# The new Sydney Fish Market - Security Risk Assessment Report

The new Sydney Fish Market

Client: UrbanGrowth NSW Development Corporation

ABN: 41 163 782 371

Prepared by

**AECOM Australia Pty Ltd**

Level 21, 420 George Street, Sydney NSW 2000, PO Box Q410, QVB Post Office NSW 1230, Australia  
T +61 2 8934 0000 F +61 2 8934 0001 www.aecom.com  
ABN 20 093 846 925

02-Apr-2018

Job No.: 60552556

AECOM in Australia and New Zealand is certified to ISO9001, ISO14001 AS/NZS4801 and OHSAS18001.

© AECOM Australia Pty Ltd (AECOM). All rights reserved.

AECOM has prepared this document for the sole use of the Client and for a specific purpose, each as expressly stated in the document. No other party should rely on this document without the prior written consent of AECOM. AECOM undertakes no duty, nor accepts any responsibility, to any third party who may rely upon or use this document. This document has been prepared based on the Client's description of its requirements and AECOM's experience, having regard to assumptions that AECOM can reasonably be expected to make in accordance with sound professional principles. AECOM may also have relied upon information provided by the Client and other third parties to prepare this document, some of which may not have been verified. Subject to the above conditions, this document may be transmitted, reproduced or disseminated only in its entirety.

## Quality Information

Document     The new Sydney Fish Market - Security Risk Assessment Report

Ref            60552556


                \\ausyd1fp001\Projects\605X\60552556\6. Draft Docs\6.1 Reports\Security

Date           02-Apr-2018

Prepared by   Krish Chammala

Reviewed by   Daniel Rasins

### Revision History

Rev	Revision Date	Details	Authorised	
			Name/Position	Signature
01	31-Aug-2018	For Review	Gus Nainu/ Practice Lead - Building Services	
02	01-Nov-2018	For Review	Gus Nainu Practice Lead - Building Services	
03	02-Apr-2019	For Issue	Daniel Fettell Principal Engineer	

## Table of Contents

Executive Summary	i
1.0 Introduction	1
1.1 Objective	1
1.2 Methodology	1
2.0 Security Standards	2
2.1 General	2
2.2 Australian / International Standards	2
3.0 Security Theories & Principles	3
3.1 General	3
3.2 Defence in Depth	3
3.2.1 Outer Layer	3
3.2.2 Middle Layer	4
3.2.3 Inner Layers	4
3.3 Deter, Detect, Delay & Response (D <sup>3</sup> R) Principle	4
3.3.1 Deter	4
3.3.2 Detect	4
3.3.3 Delay	4
3.3.4 Response	4
3.3.5 D <sup>3</sup> R Control Examples	5
3.4 Target Hardening	7
4.0 Crime Prevention through Environmental Design (CPTED)	8
4.1 CPTED Theory	8
4.2 Natural Surveillance	8
4.3 Natural Access Control	8
4.4 Territorial Reinforcement	8
5.0 Security Risk Management	9
5.1 Overview	9
5.2 Principles	10
5.3 Framework	11
5.3.1 General	11
5.4 Mandate and Commitment	11
5.5 Process	11
6.0 Information Security Management	13
6.1 Overview	13
6.2 Information Security Requirement	13
6.3 How to Establish Information Security Requirements	13
6.4 Information Security Controls	14
6.5 Critical Success Factors	14
7.0 Business Continuity Management	16
7.1 Overview	16
7.2 Business Continuity Management Definition	16
7.3 Key Elements of BCM	16
7.4 Interrelationship between Security Risk and Business Continuity Management	18
8.0 Emergency Management Planning	20
8.1 Overview	20
8.2 Emergency Identification and Analysis	20
8.3 Key Considerations	21
9.0 Security Risk Assessment	22
9.1 Communication & Consultation	22
9.1.1 Security Risk Assessment Workshop	22
9.2 Context Establishment	22
9.2.1 External Context	22
9.3 Risk Identification	25
9.3.1 Definition of Risk	25
9.3.2 General	25



	9.3.3	Identified Assets	25
	9.3.4	The Facility Assets and Resources	26
	9.3.5	Sources of Threat	27
	9.3.6	Crime Hot Spots	28
	9.3.7	Most Prevalent Crimes	29
	9.3.8	Crime Analysis	29
9.4		Risk Assessment	30
	9.4.1	Process	30
	9.4.2	Risk Assessment Matrices	30
	9.4.3	Security Risks	32
9.5		Threat Assessment	34
	9.5.1	Threat Overview	34
	9.5.2	Intent	34
	9.5.3	Capability	35
	9.5.4	Measuring the Threat	35
9.6		Risk Analysis	35
	9.6.1	Risk Trend: Terrorist Type Activities	35
	9.6.2	Risk Trend: Trespass	38
	9.6.3	Risk Trend: Theft	39
	9.6.4	Risk Trend: Antisocial Behaviour	40
	9.6.5	Risk Trend: Assault	41
9.7		Risk Evaluation	41
	9.7.1	General	41
	9.7.2	Tolerance of Risk	41
9.8		Risk Treatment	42
9.9		Monitoring & Review	42
	9.9.1	Monitoring & Review Practices	43
	9.9.2	Triggering Monitoring & Review Processes	44
	9.9.3	Post Event Analysis & Reporting	44
10.0		Recommendations	46
10.1		Overview	46
10.2		Environment Specific Considerations	46
10.3		Site Wide Recommendations	46
	10.3.1	Security Risk Management Policies and Procedures	46
	10.3.2	Security Management, Policies and Procedures	48
	10.3.3	Business Continuity Management	48
	10.3.4	Emergency Management	51
	10.3.5	Information Security	56
	10.3.6	Physical Security Measures	59
	10.3.7	Electronic Security Measures	60
	10.3.8	Personnel Security Measures	60
10.4		Public Realm	62
	10.4.1	Passive Security Measures (CPTED)	62
	10.4.2	Vegetation Maintenance Strategy	62
	10.4.3	Electronic Security Measures	63
	10.4.4	Physical Security Measures	63
10.5		Conclusion	64
Appendix A			
		Security Risk Matrix	A
Appendix B			
		Security Treatment Matrix	B

## Executive Summary

### Objectives of this Report

This Security Risk Assessment (SRA) report for The new Sydney Fish Market redevelopment The new Sydney Fish Market aims to meet the requirements the Project Scope, that addresses the identified risks including criminal activity and potential security threats.

This report provides an overview of the foreseeable security risks faced by The new Sydney Fish Market precinct and provides recommendations on possible security treatment measures that could be implemented where appropriate, in order to lower the risk profile of the precinct including operations, wholesale, critical infrastructure and public realm.

The objective of this report is to protect and preserve people, property and information within The new Sydney Fish Market precinct by identifying, assessing, evaluating and treating security related risks.

This report is intended to be a guiding document for the detailed design for the Security design and services.

### Methodology

This SRA report has been based on the International Risk Management Standard ISO 31000:2009 – Risk Management – Principles and Guidelines, and the Australian Standard Handbook HB 167:2006 Security Risk Management.

Refer to Section 1.1 for a detailed explanation of the methodology followed when producing this report.

### Findings

Refer to Appendix A for complete information regarding the identified security risks, and their ratings.

The crime levels experienced within the City of Sydney Local Government Area (LGA), Glebe Suburb in particular, within which The new Sydney Fish Market precinct will be located, are reasonably **Stable** (Source: NSW Bureau of Crime Statistics and Research). This can be partially attributed to the fact that LGA is committed to ensuring the area is safe for business and living by actively engaging local community and partnering with Local Area Commands in developing and implementing programs that address community safety and crime prevention.

In the most recent three-year crime trend data for the City of Sydney LGA, shows that ten (10) most prevalent crimes applicable to The new Sydney Fish Market are either stable or declined over this period, Based on these trends, the likelihood of these offences occurring in the future should either remain the same as currently assessed, or reduce.

The following is a list of the most prevalent offences to occur in the City of Sydney LGA that are relevant to The new Sydney Fish Market;

- Robbery;
- Theft;
- Assault (Non-domestic violence related);
- Malicious Damage to Property;
- Liquor Offences; and
- Drug Offences.

## Key Recommendations

The security risk treatment and mitigation methods recommended within this report are based on Australian Security Standards, current security trends and reasonable industry practices.

Refer to Section 10.0 for detailed recommendations to help mitigate and treat the identified security risks that The new Sydney Fish Market are exposed to.

Recommended security treatment measures include, but not limited to the following;

- Develop, implement and maintain Security Management Plans, Policies, and Procedures;
- Develop, implement and maintain Security Risk Management Plans, Policies, and Procedures;
- Develop, implement and maintain Business Continuity Management Plans, Policies, and Procedures;
- Develop, implement and maintain Emergency Management Plans, Policies, and Procedures;
- Where practical, Crime Prevention through Environmental Design (CPTED) principles will be incorporated into the detailed design, and where appropriate, maintain the facility in a way in which the CPTED aspects are enhanced or maintained in future;
- The deployment of electronic security measures to provide surveillance, detection, deterrence, and to electronically control access into and out of restricted spaces;
- Develop, implement and maintain cash handling policies and procedures to ensure that uniform, secure and best industry practices are implemented;
- Implement physical security measures to physically control/restrict access to restricted areas of the precinct and throughout the precinct including Hostile Vehicle Mitigation (HVM); and
- Implement personnel security measures such as on-site security personnel during trading hours and over peak periods, staff and contractor pre-employment screening, and security awareness training(s).

## Caveat

This security risk assessment has been based on information available at the time of writing. As risks can change rapidly it is recommended that The new Sydney Fish Market and the operator regularly review the risk profile from time to time and act accordingly.

## 1.0 Introduction

### 1.1 Objective

The objective of this SRA report is for security related safety issues and risks to be identified, analysed, and evaluated for The new Sydney Fish Market development, and to provide detailed treatment recommendations in order to lower the security risk profile of The new Sydney Fish Market complex.

### 1.2 Methodology

This SRA report has been based on the International Risk Management Standard ISO 31000:2009 – Risk Management – Principles and Guidelines, and the Australian Standard Handbook HB 167:2006 Security Risk Management.

The methodology used to create this Security Risk Assessment Report for The new Sydney Fish Markets redevelopment project entails the following steps:

- Perform a review of current project documentation in order to establish the context of the SRA including internal and external environmental factors;
- Review and analyse the Local Government Area crime statistics within which The new Sydney Fish Market is located, in order to identify the key security related risks that the precinct is exposed to;
- Review and analyse the Australian Government Census information in order to gain an understanding of the suburb demographics, to establish the internal and external environment within which the precinct is located and operates in;
- Produce a Draft Security Risk Assessment Report, including CPTED review;
- Report to provide recommendations for CPTED strategies, and physical, electronic and procedural security mitigation treatments for the identified assets;
- Undertake a SRA Workshop with key project Stakeholders to identify, analyse and evaluate/rate the security risks;
- During this Workshop the final risk ratings will be agreed upon by the Stakeholders;
- The modified risk ratings from the SRA Workshop will be incorporated into the Draft Security Risk Assessment Report, and the updated Draft Report will be issued for client comment;
- Once reviewed by the relevant Stakeholders, any comments will be reviewed and incorporated where required;
- A final Security Risk Assessment Report will then be issued to the Client;
- Project stakeholders will be liaised with throughout the SRA process; and
- The security risks faced by The new Sydney Fish Market precinct should be regularly monitored and reviewed by the relevant parties, particularly when any additional capital works projects are to be conducted in and around the facility, and when any high risk or high profile events are held within the complex or prior to the busy trading periods such as Christmas eve and New Year.



## 2.0 Security Standards

### 2.1 General

The security risk treatment and mitigation measures implemented for The new Sydney Fish Market should comply with the following standards, guidelines and handbooks;

### 2.2 Australian / International Standards

- ISO 31000:2009: International Standard for Risk Management;
- HB 167 – 2006: Security Risk Management Handbook;
- HB 327 Communicating and Consulting About Risk;
- HB 221:2004 Business Continuity Management;
- HB 292 A Practitioners Guide to Business Continuity Management;
- HB 293 Executive Guide to Business Continuity Management;
- Australian Government Protective Security Policy Framework (PSPF);
- AS 4806: Closed Circuit Television (Parts 1 – 4);
- NSW Government Policy Statement and Guidelines for the Establishment and Implementation of Closed Circuit Television (CCTV) in Public Spaces;
- AS 2201: Intruder Alarm Systems (Parts 1 – 4);
- AS 4421: Guards and Patrols;
- AS 1725: Chain-link Fabric Security Fences and Gates;
- BS 1722-10: Fences – Part 10: Specification for anti-intruder fences in chain link and welded mesh;
- BS 1722-12: Fences – Part 12: Specification for Steel Palisade Fences;
- British Standard PAS 68 – Specification for vehicle security barriers;
- Australian Government – Comcare: Prevention and Management of Customer Aggression – A Guide for Employers;
- The National Construction Code (NCC);
- AS 1428.1-2009 Design for Access and Mobility. Part 1: General Requirements for Access – New Building Work;
- AS/NZS ISO/IEC 27001:2013 Information technology - Security techniques - Information Security Management Systems – Requirements;
- AS/NZS ISO/IEC 17799:2006 Information technology - Security techniques – Code of Practice for Information Security Management;
- AS 3745-2010 Planning for Emergencies in Facilities;
- AS 5050 Business Continuity – Managing Disruption – Related Risk;
- AS 4811-2006 Employment Screening;
- PAS 68:2013 – Impact test specifications for vehicle security barrier systems;
- International Workshop Agreement (IWA) 14-1: 2013 Part 1: Performance Requirement, vehicle impact test method and performance rating; and
- International Workshop Agreement (IWA) 14-1: 2013 Part 2: Application.

## 3.0 Security Theories & Principles

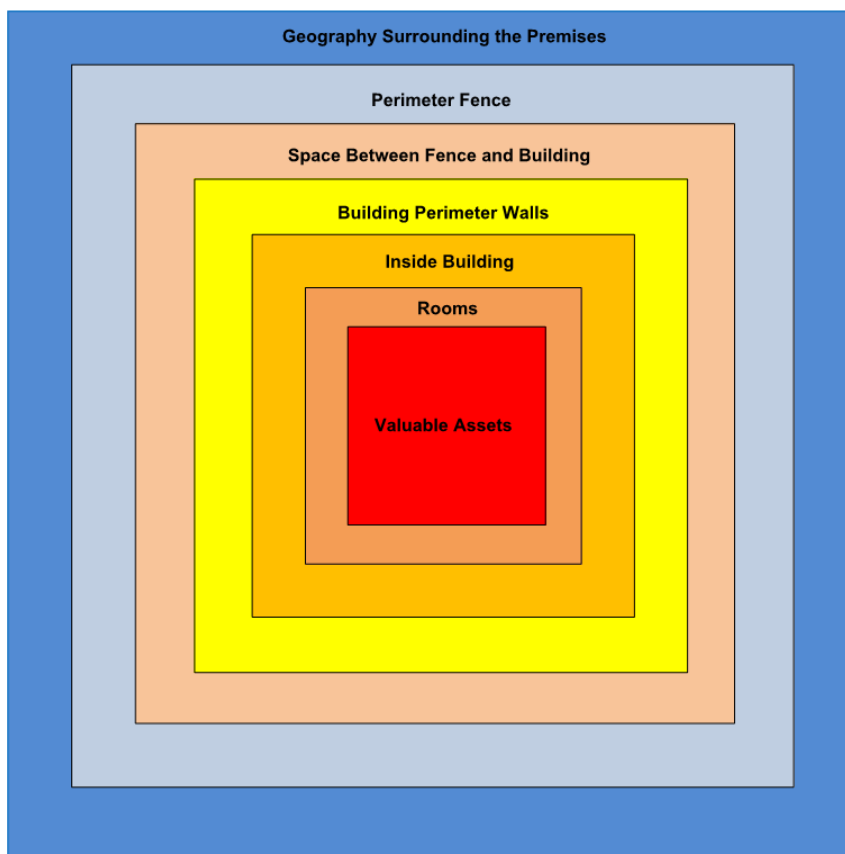
### 3.1 General

The security philosophies and principles outlined below form the basis of the security strategies and recommendations contained within this report.

### 3.2 Defence in Depth

The underlying purpose of the Defence in Depth principle 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.

The figure below illustrates the conceptual presentation of the Defence in Depth principle;



**Figure 1 Defence In Depth Diagram**

The Defence in Depth principle should be used in conjunction with the D<sup>3</sup>R security principle, outlined in Section 3.3.

#### 3.2.1 Outer Layer

Physical controls at the outer protective layer or perimeter consist of fencing or other barriers, protective lighting, signs, and intrusion detection and video surveillance. It is the outermost point at which physical security measures are used to deter, detect, delay and respond (or defend) against illegitimate and unauthorised activities. Controls at this layer are designed to define the property line and channel people and vehicles through designated and defined access points. Intruders or casual

trespassers will notice these property definitions and may decide not to proceed to avoid trespassing charges or being noticed.

The outer perimeter provides the earliest opportunity for detection and identification of intrusions.

The precinct is currently being designed accentuating natural distance to increase an intruder's perception of risk of surveillance and segregating parking facilities from unauthorised access.

### **3.2.2 Middle Layer**

The middle layer, at the exterior of buildings on the site consist of protective lighting, intrusion detection systems, video surveillance, locks, bars on doors and windows, signs, and barriers such as doors and the façade of the building itself. Protection of ventilation ducts, hatches and other miscellaneous services penetrations will also be considered during detailed design, depending on the risk profile. Intrusion detection will be provided internally to increase the effectiveness of security. Loading, unloading, sales, wholesale and auction areas will be segregated physically and electronically.

### **3.2.3 Inner Layers**

Usually, several layers are established. Their placement is designed to address an intruder who penetrates the outer and middle protective layers. The following physical controls will be designed at this layer: window and door bars, mechanical locks, electronic locks, barriers, signs, intrusion detection systems, video surveillance and protective lighting.

Areas which are deemed as high-risk and critical infrastructure i.e. plant rooms, generator rooms, and the like will be provided with electronic access control and intruder detection system.

## **3.3 Deter, Detect, Delay & Response (D<sup>3</sup>R) Principle**

The D<sup>3</sup>R 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.

### **3.3.1 Deter**

The purpose of the deter function in this strategy is to incorporate a variety of measures that can be used to deter opportunistic crime from occurring by increasing the perceived risk of detection or effort required to commit the crime.

Security methods such as signage, appropriate lighting levels, video surveillance and natural distance and surveillance (where practical) will deter opportunistic crime from occurring. Security patrols could also be considered in order to deter crime from occurring within The new Sydney Fish Market precinct.

### **3.3.2 Detect**

In order to minimise the loss or damage of assets, it is important to be able to detect unauthorised access into a protected area. The detection function of the D<sup>3</sup>R security principle will be achieved by installing and using passive infrared (PIR) volumetric detectors in nominated locations, and installing and monitoring CCTV. The precinct will be designed with appropriate illumination levels which would also significantly enhance the ability to provide the detection function.

### **3.3.3 Delay**

When unauthorised access to a facility has occurred, it is important to delay the progress of the intruder to prevent and minimise the loss or damage of assets. This delay can be achieved through a series of barriers such as mechanical locks, electronic locks, doors, windows and walls. Ideally the length of delay should be greater than the time for a response force to arrive, in order to apprehend the offenders before they reach the asset or leave the facility with the asset.

### **3.3.4 Response**

A timely and appropriate response is required at The new Sydney Fish Market by in-house and/or contract security or the local Police, depending on the nature of the event.

### 3.3.5 D³R Control Examples

Tables 1 and 2 list examples of security controls that may be utilised throughout the facility where appropriate, and details how each control fits into the D³R strategy. In addition to the Deter, Delay, Detect, and Response functions, an additional function – Recover has also been provided.

		Deter	Delay	Detect	Response	Recover
Physical Controls	Signage	Yes	No	No	No	No
	Perimeter barriers	Yes	Yes	No	No	No
	Uniformed security patrols	Yes	Yes	Yes	Yes	No
	Covert Security patrols during peak trading hours, days.	Partial	Yes	Yes	Yes	No
	Proximity to local traffic (pedestrian and vehicle)	Yes	Partial	Partial	Partial	No
	Open lines of sight (absence of building or terrain cover)	Yes	No	Yes	No	No
	Area lighting conditions	Yes	No	Yes	No	No
	Perimeter barriers	Yes	Yes	No	No	No
	Gating systems	Yes	Yes	Partial	No	No
	Building materials	Partial	Yes	No	No	No
	Vehicle control points	Yes	Yes	Yes	No	No
	Buffer zones	Partial	Yes	No	Yes	No
	Personnel screening	Partial	No	Yes	No	No
People Controls	Employee awareness program	Yes	No	Yes	No	No
	Entry searches	Yes	No	Yes	No	No
	Employee termination procedure	Yes	No	No	Yes	No
	Staff training	Yes	Yes	Yes	Yes	Yes
	Personnel movement	Yes	Yes	Yes	Partial	No
	Ethical frameworks and monitoring	Yes	Partial	Yes	No	No

**Table 1 Physical and People Security Controls**

		Deter	Delay	Detect	Respond	Recover
	Identity cards	Partial	No	Yes	No	No
	Law enforcement response	Partial	No	No	Yes	No
	Management supervision	Yes	Yes	Yes	No	No
Policy and Process Controls	Risk management	Partial	Partial	Partial	Partial	Partial
	Inventory control systems	Yes	Yes	Yes	No	No
	Internal audit and other assurance practices	Partial	Partial	Partial	Partial	Partial
	Lock-key practices	No	Yes	No	No	No
	Housekeeping	No	Partial	Yes	Partial	No
	Evacuation plans	No	No	No	Yes	No
	Process design	Yes	Yes	Yes	Yes	Yes
	Authorisation and delegation governance	Yes	Yes	Yes	No	No
	Policy framework	Partial	Partial	Partial	Partial	Partial
	Emergency management planning	No	No	No	Yes	Partial
	Business continuity management	No	No	No	Yes	Yes
	Corporate governance	Yes	Yes	Yes	Partial	Partial
	Document control	No	Yes	Partial	Partial	No
	Communications and public affairs policies and practices	No	No	Partial	No	No
	Prior publicised responses to security breaches	Yes	No	No	No	No
	Security access systems	Yes	Yes	Partial	No	No
Technology Controls	Intrusion detection and alarms	Yes	No	No	No	No
	Password and encryption keys	Yes	Yes	No	No	No
	Mail screening	Yes	No	Yes	No	No
	Surveillance capability	Yes	No	Yes	No	No
	Panic alarms	No	No	No	Yes	No

Table 2 Policy, Process and Technology Security Controls

### 3.4 Target Hardening

The aim of target hardening is to make target areas less vulnerable and increasing the time and effort required to reach the desired asset(s) within a specific area.

Target hardening measures that can be implemented throughout The new Sydney Fish Market precinct are the use of;

- High security fencing and/or barriers;
- Electronic locks and keying systems;
- Limiting miscellaneous openings on building perimeters and treating any large openings with security grilles, tamper resistant fasteners etc.;
- Electronic intrusion detection and access control systems; and
- Video Surveillance of specific areas.



## 4.0 Crime Prevention through Environmental Design (CPTED)

### 4.1 CPTED Theory

Crime Prevention through Environmental Design (CPTED) is the use of design and space management principles in order to manipulate human behaviour. The design of a particular space has to ensure that the intended activity can function properly, as well as directly supporting the control of behaviour, in order to reduce the opportunity for crime. The design of the precinct should strive to incorporate the three overlaying CPTED strategies – Natural Access Control, Natural Surveillance and Territorial Reinforcement.

### 4.2 Natural Surveillance

The intent of Natural Surveillance is to keep intruders under observation through the use of an open design with clear sight lines. Natural Surveillance increases the perception of risk of detection if the offender was to enter that particular area.

In order to maximise natural surveillance at The new Sydney Fish Market site, the design and layouts should strive to achieve where practical, clear sight lines, reduce blind spots/ hiding places/ places for concealment, use low height vegetation, position high risk areas in areas with good natural surveillance, and provide reasonable illumination to key areas.

### 4.3 Natural Access Control

The intent of Natural Access Control is to prevent access to a particular area and to create the perception of risk of detection by an offender if entering that area. Natural Access Control attempts to achieve this intent by delineating between public and private space by using the surrounds to limit or control the natural movement of persons throughout an area. Natural Access Control also aims to increase the effort required by an offender to bypass the natural barriers.

Natural access control could be implemented at The new Sydney Fish Market site by providing a clear definition of controlled space with boundaries, markings, and signage, and using lighting and landscaping to limit access or control pedestrian traffic direction and flow.

### 4.4 Territorial Reinforcement

Territorial reinforcement is the design of a particular area to create a sense of territoriality and sense of ownership by the approved users. This territoriality produces a perceived increase risk of detection to an unauthorised user.

By creating this sense of ownership, approved users of a space develop a vested interest in that space and are then more likely to challenge intruders and report them to the onsite security presence. This sense of owned space also creates an environment where 'unauthorised users' or 'intruders' stand out which creates a perceived increase in the risk of detection.

Territorial reinforcement can be incorporated into The new Sydney Fish Market site by appropriately maintaining the site, keeping it clean and tidy, and well presented. Any graffiti, vandalism and maintenance issues should be promptly dealt with to ensure the site is perceived as a highly valued space.

A separate detailed report '*CPTED Report The new Sydney Fish Market*' by AECOM has been provided for the CPTED recommendations.

## 5.0 Security Risk Management

### 5.1 Overview

The purpose of Security Risk Management (SRM) is to identify, quantify, and prioritise risks against criteria for risk acceptance and objectives relevant to the organisation (in this case The new Sydney Fish Market and its security operator). The results of a risk assessment should guide and determine the appropriate management action and priorities for managing security risks and for implementing controls selected to protect against these risks.

Risk assessment include the systematic approach of estimating the magnitude of risks (risk analysis) and the process of comparing the estimated risks against risk criteria to determine the significance of the risks (risk evaluation).

Risk assessments should also be performed periodically to address changes in the security requirements and in the risk situation, e.g. in the assets, threats, vulnerabilities, impacts, the risk evaluation, and when significant changes occur. These risk assessments should be undertaken in a methodical manner capable of producing comparable and reproducible results.

The potential benefits achievable from implementing and maintaining a Security Risk Management Plan in accordance with the International Standard ISO 31000 includes:

- Increase the likelihood of achieving objectives;
- Encourage proactive management;
- Be aware of the need to identify and treat risk throughout the organisation/Facility/Precinct;
- Improve the identification of opportunities and threats;
- Achieve compatible risk management practices;
- Comply with relevant legal and regulatory requirements and international norms;
- Improve financial reporting;
- Improve governance;
- Improve stakeholder confidence and trust;
- Establish a reliable basis for decision making and planning;
- Improve controls;
- Effectively allocate and use resources for risk treatment;
- Improve operational effectiveness and efficiency;
- Enhance health and safety performance as well as environmental protection;
- Improve loss prevention and incident management;
- Minimise losses;
- Improve organisational learning; and
- Improve organisational resilience.

This SRA report is intended to meet the needs of a wide range of stakeholders including:

- Those accountable for achieving objectives and therefore ensuring that risk is effectively managed within the facility as a whole or within a specific area or activity;
- Those responsible for developing risk management policy for the new Sydney Fish Market complex;
- Those who need to evaluate an facilities' effectiveness in managing risk; and

- Developers of standards, guides, procedures, and codes of practice that in whole or in part set out how risk is to be managed within the specific context of these documents.

## 5.2 Principles

For risk management to be effective within The new Sydney Fish Market precinct the security operator should endeavour to comply with the principles below:

- **Risk management creates and protects value.**

Risk management contributes to the demonstrable achievement of objectives and improvement of performance in, for example, human health and safety, security, legal and regulatory compliance, public acceptance, environmental protection, product quality, project management, efficiency in operations, governance and reputation.

- **Risk management is an integral part of all organisational processes.**

Risk management is not a stand-alone activity that is separate from the main activities and processes of the organisation/Facility/Precinct. Risk management is part of the responsibilities of management and an integral part of all organisational precinct processes, including strategic planning and all project and change management processes.

- **Risk management is part of decision making.**

Risk management helps decision makers make informed choices, prioritise actions and distinguish among alternative courses of action.

- **Risk management explicitly addresses uncertainty.**

Risk management explicitly takes account of uncertainty, the nature of that uncertainty, and how it can be addressed.

- **Risk management is systematic, structured and timely.**

A systematic, timely and structured approach to risk management contributes to efficiency and to consistent, comparable and reliable results.

- **Risk management is based on the best available information.**

The inputs to the process of managing risk are based on information sources such as historical data, experience, stakeholder feedback, observation, forecasts and expert judgement. However, decision makers should inform themselves of, and should take into account, any limitations of the data or modelling used or the possibility of divergence among experts.

- **Risk management is tailored.**

Risk management is aligned with the organisations/Facility's/the precincts' external and internal context and risk profile.

- **Risk management takes human and cultural factors into account.**

Risk management recognises the capabilities, perceptions and intentions of external and internal people that can facilitate or hinder achievement of the organisation's/Facility's/the Precincts' objectives.

- **Risk management is transparent and inclusive.**

Appropriate and timely involvement of stakeholders and, in particular, decision makers at all levels of The new Sydney Fish Market operations, wholesale and tenancies groups will help ensure that risk management remains relevant and up-to-date. Involvement also allows stakeholders to be properly represented and to have their views taken into account in determining risk criteria.

- **Risk management is dynamic, iterative and responsive to change.**

Risk management continually senses and responds to change. As external and internal events occur, context and knowledge change, monitoring and review of risks take place, new risks emerge, some change, and others disappear.

- **Risk management facilitates continual improvement of the organisation.**

Organisations should develop and implement strategies to improve their risk management maturity alongside all other aspects of their organisation.

## **5.3 Framework**

### **5.3.1 General**

The success of risk management will depend on the effectiveness of the management framework providing the foundations and arrangements that will embed it throughout the organisation at all levels. Risk management should be integrated into an organisations' overall management system, and adapted to meet its specific needs.

The framework assists in managing risks effectively through the application of the risk management process at varying levels and within specific contexts of the organisation.

The framework ensures that information about risk derived from the risk management process is adequately reported and used as a basis for decision making and accountability at all relevant organisational levels.

If an organisation's existing management practices and processes include components of risk management or if the organisation has already adopted a formal risk management process for particular types of risk or situations, then these should be critically reviewed and assessed against the International Risk Management Standard ISO 31000, in order to determine their adequacy and effectiveness.

## **5.4 Mandate and Commitment**

The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained collaboration by the senior management and tenants, as well as strategic and rigorous planning to achieve commitment at all levels. Where appropriate, The new Sydney Fish Market and the security operator should:

- Define and endorse the risk management policy;
- Align the organisation's culture and risk management policy;
- Determine risk management performance indicators that align with performance indicators of the organisation;
- Align risk management objectives with the objectives and strategies of the organisation;
- Comply with legal and regulatory requirements where necessary;
- Assign accountabilities and responsibilities at appropriate levels within the organisation;
- Allocate necessary resources to risk management;
- Communicate the benefits of risk management to all stakeholders; and
- Ensure that the framework for managing risk continues to remain appropriate.

## **5.5 Process**

The security risk management process followed as part of this SRA Report has been based on the ISO 31000 risk management process outlined in the Figure below;

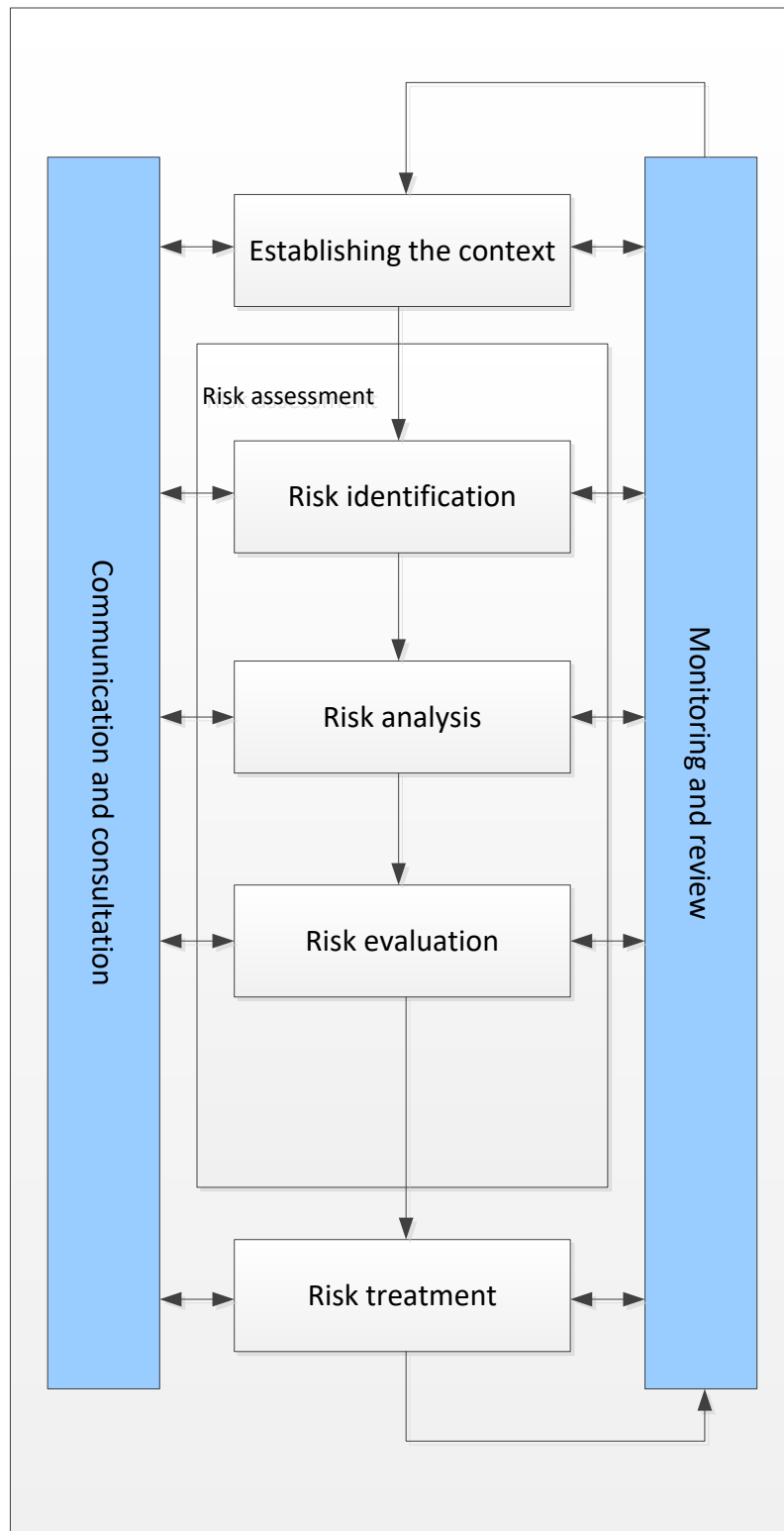


Figure 2 ISO 31000 Risk Management Process

## 6.0 Information Security Management

### 6.1 Overview

Information is an asset that, like other important business assets, is essential to an organisation's business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment. As a result of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities. It is for these reasons that The new Sydney Fish Market Facility and event information, particularly information about high profile events, auctions, requires adequate protection.

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Whatever forms the information takes, or means by which it is shared or stored, it should always be appropriately protected.

Specific attention should be made to sensitive information stored on portable electronic devices (especially personal (not company issued) devices), such as smart phones, tablets and laptops.

Information security is the protection of information from a wide range of threats in order to help ensure business continuity, minimise business risk, and maximise return on investments and business opportunities.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organisational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to help ensure that the specific security and business objectives of the organisation are met. This should be done in conjunction with other business management processes and forms part of the security risk management process.

### 6.2 Information Security Requirement

Information and the supporting processes, systems, and networks are important business assets. Defining, achieving, maintaining, and improving information security may be essential to maintain competitive edge, cash flow, profitability, legal compliance, and commercial image.

Organisations and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Causes of information damage such as malicious code, computer hacking, and denial of service attacks have also become more common, more ambitious, and increasingly sophisticated.

Information security is important to both public and private sector businesses, and to protect critical infrastructures. In both sectors, information security will function as an enabler, e.g. to achieve e-government or e-business, and to avoid or reduce relevant risks. The interconnection of public and private networks and the sharing of information resources increase the difficulty of achieving access control. The trend to distributed computing has also weakened the effectiveness of central, specialist control.

Many information systems have not been designed to be secure. The security that can be achieved through technical means is limited, and should be supported by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail. Information security management requires, as a minimum, participation by all employees in the organisation. It may also require participation from, suppliers, third parties, customers or other external parties. Specialist advice from outside organisations should be considered.

### 6.3 How to Establish Information Security Requirements

It is essential that an organisation identifies its security requirements. There are three main sources of security requirements.

- One source is derived from assessing risks to the organisation, taking into account the organisation's overall business strategy and objectives. Through a risk assessment, threats to



assets are identified, vulnerability to and likelihood of occurrence is evaluated and potential impact is estimated.

- Another source is the legal, statutory, regulatory, and contractual requirements that an organisation, its trading partners, contractors, and service providers have to satisfy, and their socio-cultural environment.
- A further source is the particular set of principles, objectives and business requirements for information processing that an organisation has developed to support its operations.

## 6.4 Information Security Controls

As a starting point, information security controls should either be based on essential legislative requirements or be considered to be common practice for information security. Controls considered to be essential to an organisation from a legislative point of view include, depending on applicable legislation:

- Data protection and privacy of personal information;
- Protection of organisational records;
- Intellectual property rights.

Controls considered to be common practice for information security include:

- Information security policy document;
- Allocation of information security responsibilities;
- Information security awareness, education, and training;
- Correct processing in applications;
- Technical vulnerability management;
- Business continuity management;
- Management of information security incidents and improvements.

These controls should be considered for implementation for the Facility where practical and appropriate.

## 6.5 Critical Success Factors

The management for The new Sydney Fish Market should strive to implement the following factors, in order to help successfully implement information security practices within the complex:

- Information security policy, objectives, and activities that reflect business objectives;
- An approach and framework to implementing, maintaining, monitoring, and improving information security that is consistent with the organisational culture;
- Visible support and commitment from all levels of management;
- A good understanding of the information security requirements, risk assessment, and risk management;
- Effective marketing of information security to all managers, employees, and other parties to achieve awareness;
- Distribution of guidance on information security policy and standards to all managers, employees and other parties;
- Provision to fund information security management activities;
- Providing appropriate awareness, training, and education;
- Establishing an effective information security incident management process;

- Implementation of a measurement system that is used to evaluate performance in information security management and feedback suggestions for improvement.

## 7.0 Business Continuity Management

### 7.1 Overview

The new Sydney Fish Market must deal with change in the environments in which they operate. Change is a constant and is best dealt with proactively rather than reactively.

To maintain business continuity, which is a core obligation of good governance, organisations must therefore anticipate and adapt to such changes to avoid either abrupt or progressive failure.

Ensuring business continuity requires a variety of conventional management techniques such as strategic and business planning, continual development of products and services, retaining and acquiring customers, recruiting new staff, raising finance, acquiring technologies and constant attention to quality and efficiency.

However, ensuring business continuity also requires effective management of the organisation's risks, including the risks that arise from the possibility of disruptive events.

### 7.2 Business Continuity Management Definition

Business Continuity Management (BCM) provides the availability of processes and resources in order to ensure the continued achievement of critical objectives.

- **'Critical Objectives'**

What the organisation, project, team, individual must absolutely strive to achieve, i.e. what are the priorities and what are less important. These will ultimately direct the focus for BCM;

- **'Processes and Resources'**

The processes that will allow critical objectives to be achieved and the resources required to support those processes;

- **'Availability'**

Processes and resources must be capable and accessible; and

- **'Continued'**

The capability to achieve critical objectives needs to be sustainable in the face of future uncertainty.

### 7.3 Key Elements of BCM

BCM can assist organisations, regardless of size, to sustain good corporate governance; maintain their critical operations and services, reputation and public image.

The key elements of BCM include:

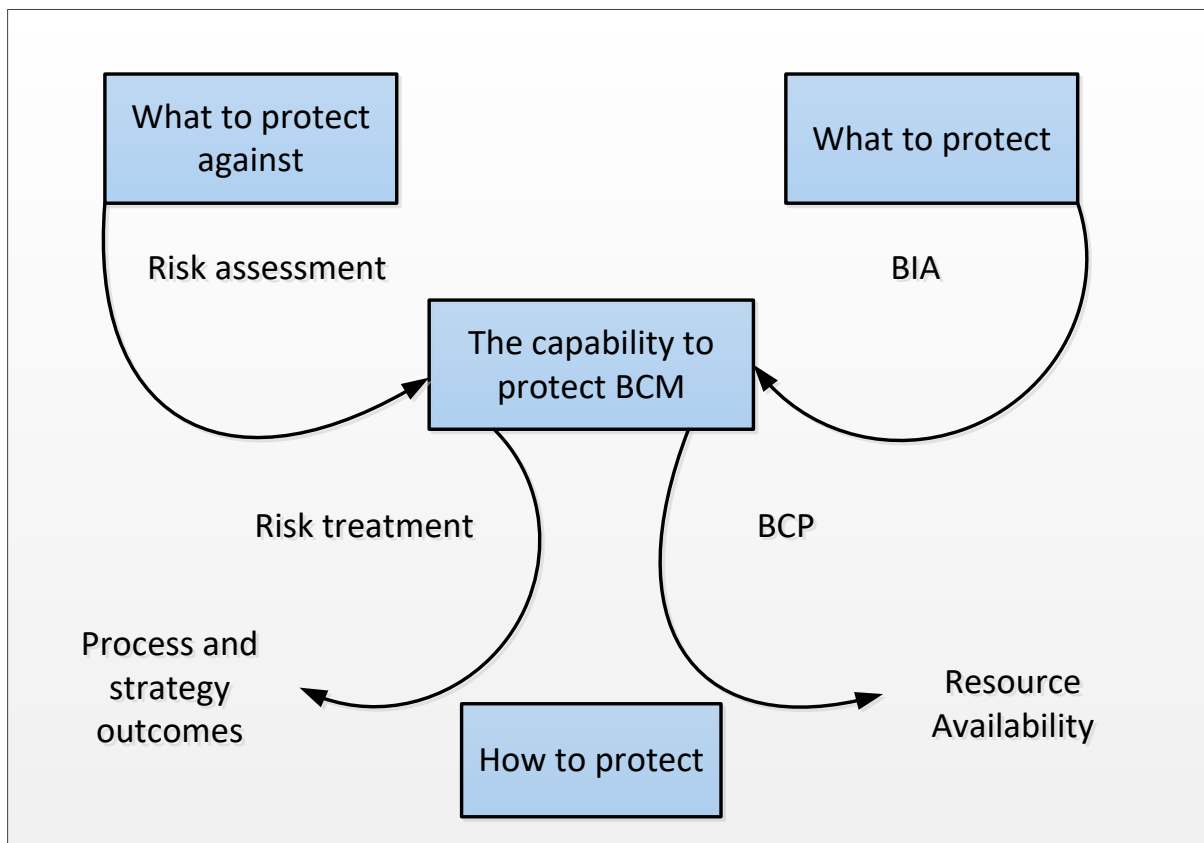
- Understanding the overall context within which the organisation operates.
- Understanding what the organisation absolutely must achieve (the critical objectives).
- Understanding what barriers or interruptions may be faced in trying to achieve these critical objectives.
- Understanding the probable outcome of controls and other mitigation strategies (remaining residual risk).
- Understanding how the organisation can continue to achieve these objectives should interruptions occur.
- Understanding the criteria or triggers for implementing crisis and emergency response, continuity response and recovery response procedures.
- Ensuring that all staff understand their roles and responsibilities when a major disruption occurs.

- Ensuring that there is a clear understanding throughout the organisation of what accountabilities and responsibilities are in place when emergency, continuity and recovery response are in effect, and that currency is maintained.
- Building consensus and commitment to the requirements, implementation and deployment of business continuity integrated as part of the routine way the site does business.

BCM is about having a robust process that allows individuals and organisations to:

- Better understand uncertainty about the future;
- Realise the potential for different types of disruption;
- Better plan for future management of those disruptions, and to put in place business improvement now to reduce the likelihood and/or consequence of significant future disruption.

The interrelationship of these elements is summarised in Figure 3 below;



**Figure 3 Key Functional Elements of BCM**

Put simply, the BCM framework illustrated in the Figure above should help the new Sydney Fish Market to answer the following questions:

- What could happen to the Facility?
- What does it mean to the Facility?
- What is critical to continuing Facility business?
- What is required to be done before, during and after an incident/event/crisis/emergency?

## **7.4 Interrelationship between Security Risk and Business Continuity Management**

Risk is present in all decisions and activities undertaken by individuals and teams within an organisation. People encounter and manage a wide variety of financial and non-financial risk on a daily basis within any type of organisation. A number of these risks will have a potentially direct impact on the continuity of the organisation.

BCM, at its most effective, should exist in a tightly bound interrelationship with risk management. The risk management process should provide the grounding for the whole BCM process: it establishes the scope, needs and priorities for BCM.

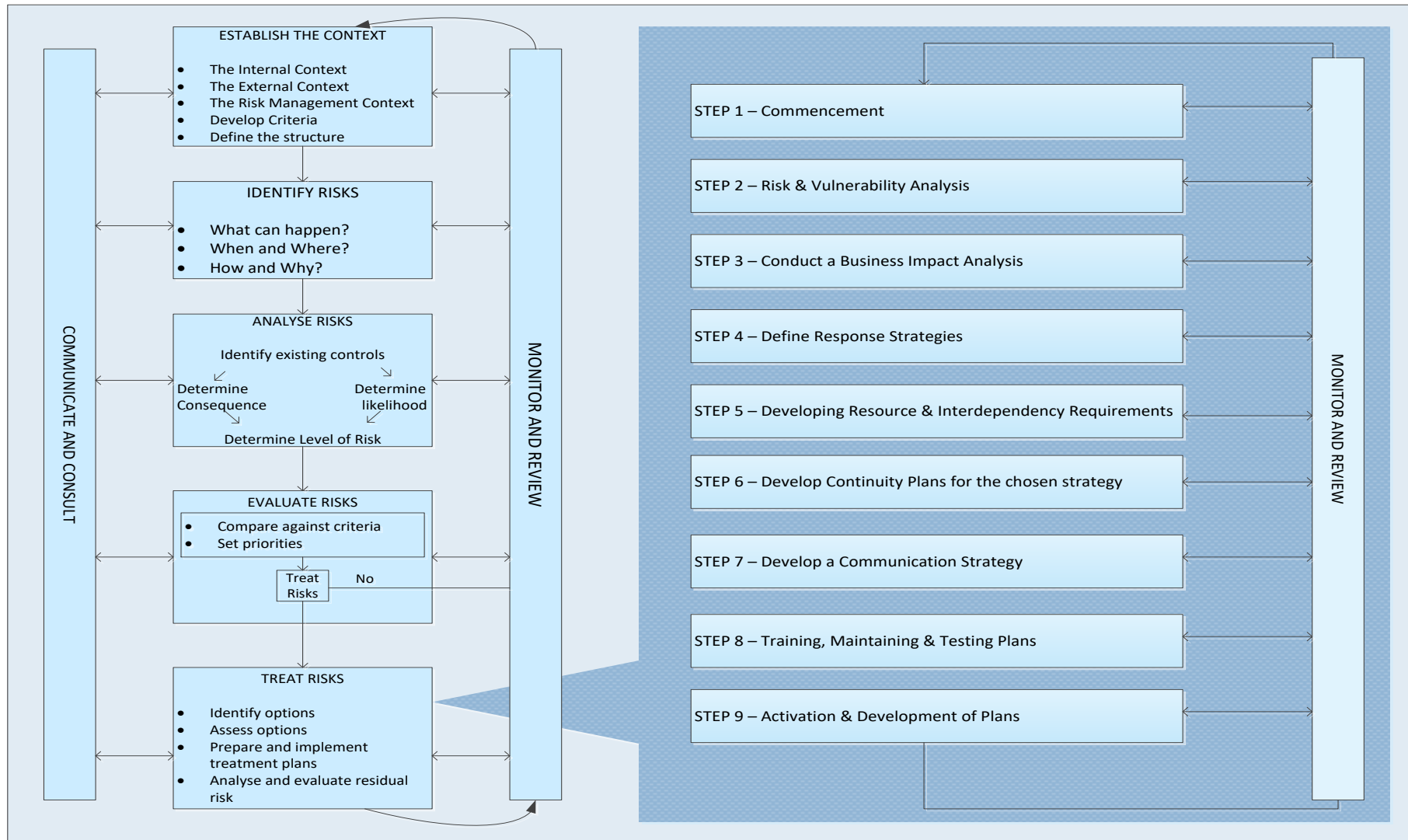
In many organisations BCM is carried out as a separate process from the risk management process. Although the outcomes from such approaches may produce adequate business continuity plans, the efficiencies and flexibility arising from a fully integrated approach may not be realised in these circumstances.

There may be valid circumstances that necessitate BCM to be conducted independently of the organisation's risk management program. However, the BCM process should still identify and assess as one of its primary steps.

Risk management and BCM need to be considered part of an integrated whole (see Figure 4 below). BCM should be conducted as one of the required outcomes of the risk management program, whilst the identification, analysis and evaluation of risk continues to be an important early step in developing the business continuity plan.

In practical terms there is commonality in the content and conduct of 'Step 1: Commencement and Context' undertaken for BCM and 'Establish the Context' for the risk management process. In an integrated approach, much of the work undertaken in the first part of the risk management process would feed directly into the start of the BCM process. With one proviso, the context is likely to be much more narrowly defined for BCM, focussing on those elements relevant to the disruption of the organisation.

Similarly, Step 2: Risk and Vulnerability Assessment, encompasses some consideration of risk management's context (through looking at vulnerabilities) and the 'Analyse Risks' step.



**Figure 4 The Interrelationship Between Security Risk Management and BCM**



## 8.0 Emergency Management Planning

### 8.1 Overview

The development and implementation of emergency plans and procedures are essential for the effective and efficient management of any emergency experienced within The new Sydney Fish Market complex.

An Emergency Plan should be developed and maintained for the site.

The Emergency Plan should document the organisational arrangements, systems, strategies and procedures relating to the response and management of emergencies. An Emergency Planning Committee (EPC) should be established for the precinct as a whole. The new Sydney Fish Market EPC should consist of key representatives from all areas i.e. The Security Operator, Operations and Wholesale.

The EPC in collaboration with the facility owners, managers, occupiers and employers should determine which types of emergencies warrant specific emergency response procedures within the emergency plan. The EPC should also consult with emergency services, particularly for high risk events.

The EPC, the management of the facility and nominated staff shall participate in the implementation and maintenance of the emergency plan, as appropriate to their role within the organisation.

#### NOTES:

- Advisors for the emergency planning process should hold recognised qualifications/competencies in a relevant discipline;
- Where security officers occupy or are engaged by a facility/precinct, their security operating procedures/site instructions should reflect, and be consistent with the emergency plan;
- The EPC should consider its emergency plan in conjunction with all emergency plans/procedures developed by neighbouring facilities (both within The new Sydney Fish Market and surrounding areas) and other relevant organisations, for example, local municipal council and Emergency Services. The use and location of the Facility may determine how the EPC will integrate its procedures with those developed by other organisations; and
- Consideration should be given to developing the emergency plan in conjunction with appropriate specialist advice, including advice on provisions for occupants with a disability.

The Emergency Plan should include, but not be limited to, the following:

- Emergency prevention;
- Emergency preparedness;
- Emergency mitigation;
- Activities for preparing for, and prevention of emergencies, such as training, and maintenance;
- Overall control and coordination arrangements for emergency response. This should include evacuation strategies for occupants with a disability; and
- The agreed roles and responsibilities of the emergency control organisation and occupants of the facility in preparation for, during and after an emergency.

### 8.2 Emergency Identification and Analysis

Identification and analysis of potential emergencies likely to impact on the precinct should be undertaken the complex as a whole including the tenants and the Cooking School to determine which events require consideration as emergencies in the Emergency Plans.

The emergency identification and analysis must include the following:

- Identifying specific emergency events and scenarios that might affect the staff and visitors.

**NOTES:**

- This should include emergency events and scenarios arising from sources:
  - Internal to the facility; and
  - External to the facility.
- The following are examples of types of emergencies to be considered:
  - Bomb threat; building invasion/armed intrusion; personal threat; chemical and biological incidents; civil disorder; medical emergency; arson, explosion; suspect object;  
Fire; cyclones, including storm surge; earthquake; explosion; fire and smoke; flood; severe weather/storm damage; and
  - Technological Hazardous substances incidents; industrial incidents; structural instability; transport incidents; toxic emissions.
- Identifying the possible consequences of each emergency to staff and visitors and their vulnerability before, during and after the emergency.
- After following the steps (a) and (b) above, deciding which types of potential emergencies are to be included in the Emergency Plan.

Potential emergencies for inclusion in the Emergency Plan may also be identified from documentation such as fire safety engineers' reports, fire safety plans, other safety reports and risk assessment reports.

### 8.3 Key Considerations

In identifying potential emergencies and developing and maintaining the Emergency Plan, the following should be taken into account:

- The size and complexity of the facility;
- Fire engineered or life safety features of the facility;

**NOTE:**

The regulatory approval process, fire engineering reports, occupant evacuation analyses, fire safety plans and other building reports should be used to determine the fire engineered or life safety features of the facility.

- Security systems, procedures and protocols;
- The number and nature of occupants, visitors, and events; and
- The hours of occupancy.

## 9.0 Security Risk Assessment

### 9.1 Communication & Consultation

Communication and consultation with internal and external stakeholders should occur at every stage of the risk management process. A stakeholder workshop will be held to discuss the security issues, to allow stakeholder input, and to agree on the security risk ratings of the identified security risks.

#### 9.1.1 Security Risk Assessment Workshop

A Security Risk Assessment workshop will be held with the relevant project Stakeholders to identify, analyse and evaluate/rate the security risks identified in Appendix A.

### 9.2 Context Establishment

#### 9.2.1 External Context

The term 'external context' refers to gaining an understanding of the external environment in which The new Sydney Fish Market is located and operating in, 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 new Sydney Fish Market or the manner in which it does business. Ultimately, the focus will be on those factors which will either directly or indirectly have security risk implications for the organisation. The outcome should be an improved understanding of the nature of external threats and opportunities that will affect security risk exposures, and the degree of uncertainty associated with those factors. In order to help to establish the external environment within which The new Sydney Fish Market is operating, this report will examine;

- The profile of the suburb of Glebe;
- The profile of its residents and nearby facilities;
- The suburb of Glebe in a political context;
- The suburb of Glebe in a socio-economical context;
- The market and infrastructure context of the suburb of Glebe; and
- The social infrastructure context of the suburb of Glebe.

#### Suburb Profile

The new Sydney Fish Market will be located within the suburb of Glebe, which is located within the close vicinity of suburb of Pyrmont and Darling Harbour Precinct.

#### Population Profile

The following statistics for the suburb of Glebe have been sourced from the 2016 Australian Bureau of Statistics and help to provide an insight into the suburb from a population point of view:

Indicator	Percentage	NSW Average
<b>Population</b>	<b>11,532 (Total)</b>	<b>N/A</b>
Males	46.7%	49.3%
Females	53.3%	50.7%
Australian Born	54.7%	65.5%
<b>Age Structure</b>		
Aged under 24 years	24.7%	31%
Aged 65+	14.1%	16.2%
<b>Birth Place</b>		
Australia	54.7%	65.5%

Indicator	Percentage	NSW Average
England	4.6%	3.0%
China	3.6%	3.1%
New Zealand	2.8%	1.6%
<b>Religion</b>		
No religion, so described	43.0%	25.1%
Catholic	17.3%	24.7%
Not stated	14.4%	9.2%
Buddhism	4.8%	2.8%
<b>Language</b>		
English Speaking Only	22.0%	23.3%
Mandarin	3.9%	3.2%
Vietnamese	2.4%	1.6%
Spanish	1.8%	0.8%
Cantonese	1.6%	1.9%

### Socio-Economic Context

The following statistics for the suburb of Sydney have been sourced from the 2011 Australian Census, and help provide an insight into the suburb from a socio-economic point of view:

Indicator	Percentage	Sydney Average
<b>Education</b>		
University or Tertiary Institution	34.6%	16.2%
Technical or Further Education Institution	5.4%	6.2%
Not Stated	33.2%	23%
<b>Employment Status</b>		
Employed – Full Time	60.3%	59.2%
Employed – Part Time	28.7%	29.7%
Unemployed	6.7%	6.3%
Away from Work	4.3%	4.8%
<b>Occupation</b>		
Professionals	42.1%	23.6%
Managers	15.5%	13.5%
Technicians & Trade Workers	7.1%	12.7%
Community & Personal Services Workers	9.0%	10.4%
Clerical & Administrative Workers	11.8%	13.8%
Sales Workers	7.2%	9.2%
Machinery Operators & Drivers	1.4%	6.1%
Labourers	4.3%	8.8%

Indicator	Percentage	Sydney Average
<b>Industry of Employment</b>		
Higher Education	6.5%	1.4%
Cafes, Restaurants and Takeaway Food Services	4.0%	2.4%
Hospitals	3.6%	3.5%
Computer System Design and Related Services	3.2%	1.9%
Legal Services	2.7%	1.2%
<b>Median Income (Weekly)</b>		
Personal	\$834	\$664
Family	\$2,347	\$1,780
Household	\$1,579	\$1,486
<b>Housing Tenure</b>		
Owned	16.0%	33.2%
Being Purchased	17.3%	33.4%
Renting	63.3%	30.1%
<b>Dwelling Structure</b>		
Separate House	4.9%	66.4%
Semi-detached, row or terrace house, townhouse	51.0%	12.2%
Flat, Unit, Apartment	41.8%	19.9%

### Infrastructure Context

The key infrastructure nearby The new Sydney Fish Market and within the suburb of Glebe includes;

- Glebe Light Rail;
- Ferry Wharfs;
- The Star Sydney;
- Powerhouse Museum; and
- Numerous entertainment, cultural, business, and accommodation locations and other infrastructure.

### Social Infrastructure Context

#### *Education Facilities*

The following educational institutions are located in the nearby area:

- University of Technology Sydney;
- Ultimo College TAFE;
- International Grammar School; and
- The University of Sydney.

### *Emergency Services*

#### NSW Police:

The Glebe and Sydney City Police Stations are located in the nearby area. The Glebe Police Station is located within 1.5 KM radius.

#### Fire and Rescue NSW:

Glebe, Pyrmont, Sydney and The Rocks Fire Stations are located in the nearby area.

#### Medical Services:

St. Vincent's Hospital, Royal Prince Alfred Hospital and Balmain Hospital are located in the nearby area.

## **9.3 Risk Identification**

### **9.3.1 Definition of Risk**

Risk is a measure of the likelihood of a threat being realised, resulting in harm to a person, facility or activity. Risk can be simply defined as: Risk = Likelihood x Consequence.

Likelihood refers to the chance of something happening, whether defined, measured or determined objectively, subjectively, qualitatively or quantitatively, and described using general terms or mathematically.

Consequence refers to the outcome of an event that affects objectives.

### **9.3.2 General**

The assessment of the risk is made up of identifying the risk, analysing the risk and evaluating the risk.

Risk identification involves the identification of the sources of risks, determines their causes and identifies their potential consequences. The identification of security risks should occur through a stakeholder workshop, reviewing reported security incidences and reviewing the local crime statistics for the LGA within which The new Sydney Fish Market is located.

Risk analysis refers to the process of comprehending the nature and level of risk. It provides the basis for risk evaluation and aids in the decisions about risk treatment.

Risk evaluation is a process which assists decision making based on the risk analysis outcomes. Risk evaluation identifies which risks require treatment and determines the priority for the risk treatment implementation.

### **9.3.3 Identified Assets**

The following details the main assets identified within The new Sydney Fish Market that require protection against the identified risks listed in Appendix A:

<b>People</b>
<b>People associated with the Facility</b>
• Staff
• Local Tourists
• International Tourists
• Restaurant patrons
• Cooking School tutors and students
• Commercial and Retail lessees
• Contract Service Providers, e.g. Security, Cleaners etc.
• Contractors, e.g. tradespersons
• Visitors, e.g. family and friends



• General Public
• Local and International Students from nearby Universities and TAFE
• Other external Marine students
• Retail wholesalers
• Deliveries, etc.
<b>Property and Equipment</b>
<b>The new Sydney Fish Market incorporates the following spaces</b>
• Wholesale Area
• Auction Hall
• Retail Area
• Cooking School
• Commercial Areas
• Operational and Management Offices
• Wharfs Terminal(s)
• Car parking
• Loading Dock
• Public Domain including dining and catering areas

#### 9.3.4 The Facility Assets and Resources

The following details some of the key The new Sydney Fish Market assets and resources, which also require protection against the identified risks listed in Appendix A:

<b>Security Systems and Equipment</b>
• Electronic Access Control and Intrusion Detection System
• Video Surveillance Systems including CCTV Cameras and Control Equipment
• Licence Plate Recognition System
• Duress Alarm System
• Intercoms and Help Points
• Public Address and Paging Systems
<b>Plant and Other Equipment</b>
• Mechanical & Air Conditioning systems
• Electrical Switchboard and Plant equipment
• Generator and UPS systems
• AV/ Auction Display systems and other high cost and critical technical components
• Weighing equipment, sealers and POS terminals.
• IT equipment and site wide network equipment etc.
• Furniture, Fittings and other Equipment (FFE)
<b>Precinct Management Information</b>
<b>Information classifications</b>
• Commercially sensitive information
• Staff/client and personal information

• Corporate strategies and objectives
• Security practices and procedures
• Wholesalers and personal information
• Contractual, financial, and insurance information
<b>The Facility Reputation</b>
<b>The Facility Reputation concerns</b>
• Name and integrity
• Safe and secure environment
• Public perception

### 9.3.5 Sources of Threat

The sources of threats that the facility is likely to be exposed to include:

- Trespassers (both intentional and unintentional);
- Assault (including aggressive behaviour, verbal abuse, etc.);
- Burglary (break-&-enter);
- Vandalism;
- Graffiti Artists (Taggers);
- Theft, including:
  - of property;
  - from a vehicle; and
  - of vehicle.
- People under the influence of drugs/alcohol (includes people who've entered the venue intoxicated);
- Antisocial people (people conducting themselves in a disorderly or offensive way);
- Criminals (opportunists, individuals, criminal groups, organised crime);
- Issue/Politically motivated groups (e.g. protestors, etc.)
- Disgruntled staff, contractors, members of the public; and
- People suffering from a mental health conditions.

It is important to be aware of the likely sources of threat as each source poses unique risks and each risk may be required to be treated differently in relation to each threat source (e.g. trespass by an issue motivated person poses a different risk and needs to be treated differently to trespass by a disgruntled staff member).

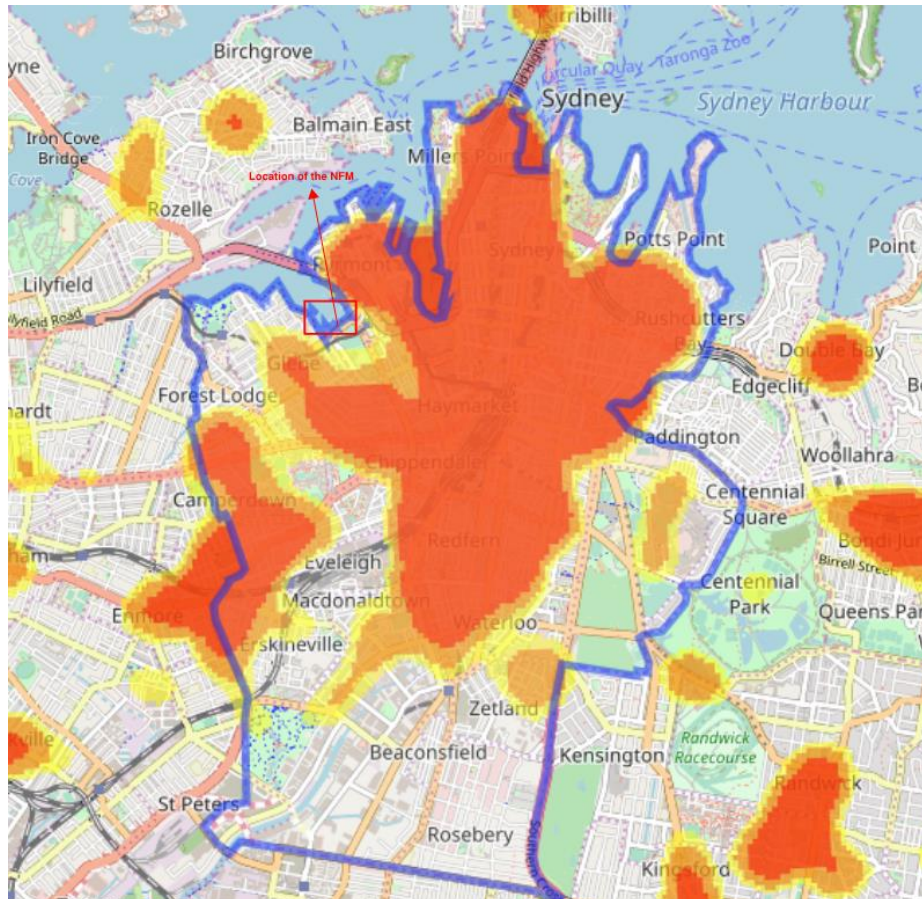
Table 3 below illustrates the objectives of each source of threat.

**Table 3 Objectives of Threat Sources**

Who (Threat)	Seek Benefits	Fun	Challenge	Revenge	Satisfy Malice	Political Advantage	Publicity	Harassment	Disruption
Issue/Politically Motivated Persons	•					•	•	•	•
Terrorists				•	•		•	•	•
Disgruntled people					•				
Antisocial People		•	•						
Mischievous people	•	•	•						
Vandals or Saboteurs		•	•	•	•			•	•
Trespassers	•		•						•
Criminals	•								

### 9.3.6 Crime Hot Spots

The map below (Figure 5 Sydney LGA Crime Hot Spots) portrays the crime hot spots for the Sydney Local Government Area;



**Figure 5 Sydney LGA Crime Hot Spots**

### 9.3.7 Most Prevalent Crimes

The following is a list of the most prevalent offences to occur in the City of Sydney LGA that are relevant to The new Sydney Fish Market. A ranking of the Sydney LGA compared to the other LGA's for each offence type cannot be provided due to the fact that its residential population does not accurately reflect the number of people present in the area each day. The most prevalent offences relevant to The new Sydney Fish Market site include:

- Theft,
- Assault (Non-domestic violence related),
- Burglary (break and enter (non-dwelling)); Malicious Damage of Property (plant, equipment and services);
- Liquor Offences,
- Disorderly Conduct (Offensive Conduct),
- Harassment, Threatening Behaviour and Private Nuisance, and

### 9.3.8 Crime Analysis

The crime levels experienced within the Sydney LGA are reasonably **Stable**. As can be seen in the five year trend table below, nine out of the ten most prevalent crimes applicable to The new Sydney Fish Market have declined over this period with the exception of drug offences. Based on these trends, the likelihood of these offences occurring in the future should either remain the same as currently assessed, or reduce.

#### 5 Year Trend

Offence	Year-March 2014	Year-March 2015	Year-March 2016	Year-March 2017	Year-March 2018	60 Month Trend	Ave Annual % Change
Theft	4653	4632	3917	3810	3552	Down	-9.3%
Assault – non-domestic violence related	3443	3170	3202	3233	3265	Down	-4.2%
Malicious damage to property	3230	2836	2747	2675	2489	Down	-9.1%
Liquor Offences	3489	2827	2900	2948	2741	Down	-8.6%
Steal from Person	2113	1888	1566	1328	1215	Down	-15.5%
Steal from motor vehicle	2244	2072	1654	1532	1195	Down	-17.1%
Disorderly Conduct	2738	2325	2258	2139	2020	Down	-10%
Break and enter non-dwelling	903	554	489	574	548	Down	-14.4%
Motor Vehicle	428	388	331	354	350	Down	-7.7%

Offence	Year-March 2014	Year-March 2015	Year-March 2016	Year-March 2017	Year-March 2018	60 Month Trend	Ave Annual % Change
Theft							
Drug Offences	7243	7931	9094	9184	9438	Up	+3.8%

## 9.4 Risk Assessment

### 9.4.1 Process

The security risk assessment process involved a desktop analysis of the relevant NSW police crime statistics for the Local Government Area of Sydney, within which The new Sydney Fish Market is located. This information is used to develop a risk profile for the site which allows likelihood and consequence values to be assigned to identified individual threat sources. This assessment is documented in Appendix A.

Following the Draft Issue of this report, a security risk workshop will be held with the relevant project stakeholders to agree on and accept the risk ratings.

The identified risks are ranked from Low to Extreme, with Low risks to be monitored for change. Any risks that fall within the categories of Medium to Extreme are addressed using various mitigation strategies. These mitigation strategies form the basis of the risk reduction recommendations.

The implementation of recommendations will be the responsibility of the relevant The new Sydney Fish Market stakeholders.

### 9.4.2 Risk Assessment Matrices

The following matrices portray the definition of each likelihood and consequence rating that has been used during the risk assessment process. Following these, the risk rating matrix table outlines how an overall risk rating is given to a particular risk, once the level of likelihood and consequence has been established.

**Table 4 Likelihood Definitions**

#### Likelihood

<b>Likelihood</b>	<b>Almost Certain</b>	Over 99% probability, or Happens often, or Could occur within days to weeks
	<b>Likely</b>	>50% probability, or Could easily happen, or Could occur within a year or so
	<b>Possible</b>	>10% probability, or Could happen/Has occurred before, or could occur within a year or so
	<b>Unlikely</b>	>1% probability, or Has not happened yet, but could, or Could occur after several years
	<b>Rare</b>	<1% probability, or Conceivable but only in extreme circumstances, or Exceptionally unlikely, even in the long term future, or A 100 year event or greater.

Table 5 Consequence Definitions

## Consequence

Consequence		People	Property & Equipment	Business Operations	Information	Reputation
	Catastrophic	Multiple deaths or fatalities	Total loss or destruction of core business property & equipment	Total cessation of services or critical business failure.	Compromise of information and total data breach.	Intense Public and media scrutiny. Eg: Local and International NEWS headlines, TV, etc
	Major	Single death or fatality	Major theft, sabotage or destruction to core business property & equipment	Cessation of service or operations, with major loss to core business operations.	Compromise of information sensitive to auction, bidding and trade	Public and media scrutiny. Eg: Local NEWS headlines, TV, etc
	Moderate	Major or Serious injury to staff, visitors (i.e. Life Threatening)	Theft or destruction to major property & equipment	Cessation of service or operations, with significant impact to core business operations.	Compromise of information sensitive to NFM, intellectual property or operations.	Strong scrutiny by external committees or agencies
	Minor	Minor Injury to staff, visitors, vendors, traders (i.e. First Aid Treatment required onsite)	Minor theft or damage to property & equipment (eg damage to vehicles or equipment, major theft of materials, etc)	Temporary cessation of services or operations, with minimal impact to core business operations.	Compromise of information sensitive to NFM interest e.g., auctions, trade details.	Internal scrutiny by senior management, internal committees or auditors to prevent escalation
	Insignificant	Nil injury to staff or visitors	Petty theft or vandalism to property & equipment (eg graffiti, defacing of property or theft of personal property)	Nil impact to service provision or operations.	Compromise of information otherwise available in the public domain.	Internal self review and improvement required

Table 6 Risk Rating Matrix and Definitions

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

Risk Level	Symbol	Definition
Extreme Risk	E	Immediate action required
High Risk	H	Senior management attention needed
Medium Risk	M	Management responsibility to be specified
Low Risk	L	Manage by routine procedures

The completed Security Risk Matrix can be found in Appendix A. The Risk Matrix identifies risk events relevant to The new Sydney Fish Market.

In the context of The new Sydney Fish Market project, this risk assessment extends primarily to the personal safety of staff, contractors and visitors. It also considers the risk, loss or compromise of The new Sydney Fish Market assets or information.

If a threat is realised by the occurrence of an adverse event, harm could result in one or more of the following categories:

- Loss of confidence in The new Sydney Fish Market and diminished reputation;
- Negative impacts on The new Sydney Fish Market's objectives;



- Partial or full disruption of The new Sydney Fish Market's services;
- Partial or complete loss of critical assets.
- Significant loss of company or personal property;
- Ongoing maintenance and repair expenses to property and assets;
- Threatened or actual violence against staff/contractors/visitors;
- Disruption to operations through staff workers compensation scheme and lost productivity; ad
- Poor staff morale.

General statistical information related to crime types was sourced from the NSW Bureau of Crime Statistics and Research (BOCSAR) relating to crime incidents that have occurred in the City of Sydney LGA. These statistics are not detailed to street level and therefore they may not provide a complete representation of historic incidents at The new Sydney Fish Market.

### 9.4.3 Security Risks

The risk events listed in the tables below are assessed as having Medium to High risk ratings and therefore require appropriate mitigation strategies to adequately treat them. These tables are a representation of the highest ranked risks, and do not include all Medium risks. Refer to Appendix A for complete list of risks.

**Table 7 Public Realm and Promenade Risks**

Risks	How It Can Be Realised	Risk Rating (Pre-treatment)	Risk Rating (Post-treatment)
Breakdown of policies and procedures for specific events	Introduction of Contraband.	High	Medium
Liquor offences	Intoxicated persons posing a risk to themselves or others.	High	Medium
Theft	Theft of equipment/assets.	High	Medium
Potential hostile vehicle attack	Risk of hostile vehicle(s) entering the public realm and/or promenade areas.	High	Medium
Drug offences	Risk of unpredictable patron behaviour due to excessive use of drugs, mental unsteadiness, violent nature.	High	Medium
Physical assault	Of staff/contractors/general public.	Medium	Medium
Vandalism / graffiti	General by criminals, opportunists, youths, gangs etc.	Medium	Medium



**Table 8 Trading Area (Wholesale and Auction) Risks**

<b>Risks</b>	<b>How It Can Be Realised</b>	<b>Risk Rating (Pre-treatment)</b>	<b>Risk Rating (Post-treatment)</b>
Liquor offences	Intoxicated persons posing a risk to themselves or others.	High	Medium
Breakdown of policies and procedures for specific events	Failure to provide necessary escape paths in emergencies.	High	Medium
Theft	Theft of cash / cheques and fraud.	High	Medium
Harm to staff and other vendors	Incidents relating to disgruntled vendors who might lose the auction. Whilst these type of incidents generally involve verbal altercations, the possibility of intensification to a physical assault is possible.	Medium	Medium
Physical assault	Risk of assault to staff working alone (lone worker situation) during night shifts, early mornings and/or working in isolated areas.	Medium	Medium
Harassment, threatening behaviour and private nuisance	Harassment, threats or demonstrations towards exhibitors/staff/contractors/general public	Medium	Medium
Unauthorised or inadvertent disclosure of sensitive information	Unauthorised or inadvertent disclosure of sensitive information (trading details, stock levels) by staff member or contractor (i.e. loose lips) resulting in loss of competitive advantage, exposure of data, etc. causing embarrassment and/or possible significant financial impact or loss.	Medium	Medium
Vandalism / graffiti	General by criminals, opportunists, youths, gangs etc.	Medium	Medium

**Table 9 Office Space and Critical Infrastructure Plant Risks**

<b>Risks</b>	<b>How It Can Be Realised</b>	<b>Risk Rating (Pre-treatment)</b>	<b>Risk Rating (Post-treatment)</b>
Property Damage	Failure to restrict access control for unauthorised access.	High	Medium
Breakdown of policies and procedures for specific events	Failure to provide necessary escape paths during emergencies.	High	Medium
Disruption of business	Disruption of business activities caused due to unauthorised access of critical infrastructure and information.	High	Medium
Theft - individual / opportunist	Theft of property, equipment or information resulting in financial loss to	Medium	Medium

Risks	How It Can Be Realised	Risk Rating (Pre-treatment)	Risk Rating (Post-treatment)
	the organisation, cessation or interruption to services, loss of personal property, embarrassment or impact to reputation, etc.		
Vandalism / graffiti	General by criminals, opportunists, youths, gangs etc.	Medium	Medium

Table 10 Car Park Risks

Risks	How It Can Be Realised	Risk Rating (Pre-treatment)	Risk Rating (Post-treatment)
Liquor offences	Intoxicated persons posing a risk to themselves or others	High	Medium
Theft	Theft of belongings, assets	High	Medium
Physical assault	Of staff/contractors/vendors/general public	Medium	Medium
Vandalism / graffiti	General by criminals, opportunists, youths, gangs etc.	Medium	Medium

## 9.5 Threat Assessment

### 9.5.1 Threat Overview

A security definition for threat is:

#### Threat = Intent X Capability

Where intent and capability refer to characteristics of individuals or groups that have the potential to do harm to another individual, organisation or community.

### 9.5.2 Intent

Intent is represented by the covert, implicit or expressed aims, goals, objectives, desires, or directions of the threat. Major components of intent comprise the motivational factors for such individuals or groups.

Traditional approaches to identifying motivational intent have focused upon an analysis of issues such as political, social issue-oriented, religious, ideological, economic, and revenge/retribution. Whilst traditionally these motivations have been regarded as discrete issues, recent international events (e.g. activities of terror groups, role of international criminal and gangs in money laundering and people smuggling) have demonstrated significant overlap and blurring amongst many of these motivating factors.

Some common forms of motivation derive from either a need for some form of self-advantage (personal benefit), or the desire to create change or gain benefit for a group, community or society at large ('altruistic' benefit). Some examples of commonly seen motivating factors are summarised in the Table below.

Personal Benefit	Altruistic Benefit
Pecuniary advantage (self and close associates)	Achieve group/ community agenda
Prevent harm or loss (self and close associates)	Gain attention on group messages
Gain attention (self-interest/ peer approval)	Influence 3rd party decisions

Personal Benefit	Altruistic Benefit
Influence 3rd party decisions	Vengeance
Seek vengeance	Punishment for perceived societal wrongs
Seek self-justification	Proxy atonement
Pathological disorders	Influence change

### 9.5.3 Capability

Capability considers the following attributes of the 'aggressor':

- Skills;
- Knowledge;
- Access to equipment (e.g. weapons, specialist equipment), finances and other resources;
- Numbers of attackers/adversaries;
- Access to support networks, time; and
- Access or opportunity that would allow the threat source (individual or group) to perpetrate an 'attack' against the target if they had the intent to do so (provision of this opportunity will also be significantly influenced by the vulnerability of the target).

By considering the types of threat and motivation, a range of credible threat scenarios can be created, and by additionally examining the threat sources' capability an initial estimate of the likelihood of the threat can be made. Historical trend data, previous incidents, intelligence (from local police crime advice/intelligence) can be used to inform the development of these scenarios.

### 9.5.4 Measuring the Threat

Threat can be measured qualitatively or quantitatively based on an understanding of the aggressors' intent and capability.

An assessment on the threat that each risk trend poses will be provided in the Risk Analysis Section below.

## 9.6 Risk Analysis

### 9.6.1 Risk Trend: Terrorist Type Activities

The Australian New Zealand Counter Terrorism Committee (ANZCTC) has provided recent advice on three specific areas of threat; 'Active Shooter Guidelines' 'Improvised Explosive Detection (IED) Guidelines for Places of Mass Gatherings' and Hostile Vehicle Guidelines for Crowded Places'.

Public events and places of mass gatherings are classified as 'soft targets'. Although, terror related activities may not directly pose a threat to the precinct, the consequence of these events could be catastrophic. This places greater emphasis on The new Sydney Fish Market preparedness to respond to a major incident, ensuring harm minimisation is a priority.

### Threat posed by Terrorist Type Activities

		<b>INTENT</b>		
		<b>Little</b>	<b>Expressed</b>	<b>Determined</b>
<b>CAPABILITY</b>	<b>Extensive</b>	Medium	High	Extreme
	<b>Moderate</b>	Low	Significant	High
	<b>Low</b>	Low	Medium	Significant

### Threat Analysis

Terrorists have been assessed as having Determined Intent, as they are perceived as having strong religious, ideological and political motivation, and well defined objectives.

Terrorists have been assessed as having Moderate capability due to the ease of access to skills, knowledge and support networks through internet research, terrorist training manuals, and websites/forums/social media. Due to the more difficult access to weapons, specialised equipment, finances and other resources, the Capability rating was not rated at Extensive.

### Risk Analysis

As can be observed in the Appendix A, terrorist based security risks pose a risk to the complex. However, it should be noted that each of these risks have been assessed as having a Rare likelihood, and that it is only due to their potential to have catastrophic consequences that has resulted in their Medium risk ratings. The Rare likelihood rating has been based on the current National Terrorism Public Alert System level, the location of the markets, and the historical occurrence of these types of events taking place in mass gathering settings within Australia.

The National Terrorism Threat level is currently (as at the date of this report) **Probable**.

The National Terrorism Threat Level System is a range of five tiers colour coded that communicate an assessed risk of terrorist threat to Australia. The five tiers are:

- **Not Expected** - Terrorist action is not expected;
- **Possible** – Terrorist action as being possible;
- **Probable** – Terrorist action is probable; and
- **Expected** – Terrorist action is expected;
- **Certain** – Terrorist attack is certain or has occurred.

The National Terrorism Threat Advisory System guides national preparation and planning. It also dictates levels of precaution and vigilance to minimise the risk of a terrorist incident occurring.

The Australian Government regularly reviews these alert levels.

According to NSW Counter Terrorism - Australia has been identified as a terrorist target in public statements by terrorist spokespeople and through terrorist planning. There has been at least one aborted, disrupted or actual terrorist attack against Australian interests every year since 2000.

The main threat to Australia comes from Islamic terrorists. However, continuing statements by ISIS leaders and other Islamic extremists also resonate with individuals not otherwise associated with

terrorist groups, who might be inspired to act. As a result, the terrorist threat to Australia will be an enduring one.

NSW Counter Terrorism also states that NSW features many of the characteristics that are attractive to contemporary terrorist organisations due to it being Australia's most populous state, the largest economy, and the fact that Sydney has a global profile.

The risks posed by these terrorist type events can be minimised through;

- State and Federal Government Departments taking over the planning and operations of events containing VVIP's.
- The development and implementation of business continuity management policies and procedures.
- The development of emergency evacuation and response policies and procedures.
- Liaison and coordination of emergency services response and strategy.
- Development of procedures to handle identified unattended/suspicious items.
- Facility fire and emergency systems designed to relevant codes and standards.
- Staff to be provided with security awareness training to increase the likelihood of detection of placed suspicious object before incident.
- Modern Video Surveillance Systems & enhanced security lighting to provide deterrence, surveillance and detection of suspicious objects/activity.
- Natural surveillance strategies to be implemented in and around the new Sydney Fish Market precinct, and throughout the precinct to maximise clear sightlines and minimise areas of concealment.
- Intruder alarm system to monitor high risk areas and detect unauthorised access.
- Electronic and physical security to control access into offices and throughout the new Sydney Fish Market precinct. Where appropriate, standoff distances to be provided through natural and physical access control measures.
- Fragmentation and secondary projectiles should be minimised where possible.
- Liaison with State/Federal Police, Security & Intelligence Agencies on a regular basis to obtain credible intelligence and Threat assessment updates on likely threat types.

### **Places of Mass Gathering**

Places of mass gathering incorporate a diverse range of facilities including, but not limited to, sporting venues, shopping and business precincts, tourism/entertainment precinct/attractions, hotels and convention centres, major events and public transport hubs.

This also includes significant one off events. They are characterised by having a large concentration of people on a predictable basis and often have a minimum of security controls present.

Places of mass gathering not only present terrorists with potential opportunities for mass casualties, symbolism and high impact media coverage, they pose a broad range of security challenges for their owners and operators.

The Australian National Counter-Terrorism Committee (NCTC) has noted that places of mass gathering have been specifically identified by religious and political extremists as attractive targets.

Facilities such as The new Sydney Fish Market are a globally tourist destination and on particular days the location can have masses of crowds particular in its retail areas and public domain.

Recently, one of the key Melbourne landmarks (Queen Victoria Market) has been identified as a potential terror target. After further assessments by the Victoria Police, National Security agencies confirmed there is no direct threat to the markets. However, places such as The new Sydney Fish Market could become a potential target due to symbolism, crowded venue and a major tourist attraction.

In 2017, Borough Market in London was targeted by terrorists which saw eight people killed in around the market food hub areas.

### 9.6.2 Risk Trend: Trespass

#### Threat posed by Trespass (Deliberate/Forced Access)

		<b>INTENT</b>		
		<b>Little</b>	<b>Expressed</b>	<b>Determined</b>
<b>CAPABILITY</b>	<b>Extensive</b>	Medium	High	Extreme
	<b>Moderate</b>	Low	Significant	High
	<b>Low</b>	Low	Medium	Significant

#### Threat Analysis

For the threat analysis, only deliberate trespass and forced access has been considered.

Trespassers have been assessed as having Little Intent, as they are perceived as having a more personal benefit motivation, such as self-interest or peer approval.

Trespassers have been assessed as having Moderate capability due to the ease of access to restricted areas through tailgating, picking locks, break-and-enter, scaling barriers etc.

#### Risk Analysis

In regards to the risk trend of trespass, the following ways in which it can be realised will be examined;

- Unauthorised (inadvertent) personnel entry into restricted areas of the facility,
- Unauthorised (inadvertent) vehicle entry into car park and loading dock areas.
- Forced unauthorised entry into restricted areas of the facility, and
- Forced unauthorised vehicle entry into car park, and loading dock areas.

The trespass types above have been rated as Medium risk.

In order to reduce the security and commercial risks posed by unauthorised access to restricted areas, high security locking devices, electronic access control, intruder alarm detection devices, and CCTV should be provided. Electronic access control and high security locking devices should be installed as a measure to control entry into restricted areas of the facilities. Good lighting levels, clear sight lines and CCTV are important treatment measures to provide surveillance of these areas. The integrity of restricted areas and/or the building perimeter should be monitored by an intruder alarm system during non-operational hours.

Security lighting, CCTV and security signage should be provided to deter illegitimate site users from entering restricted areas and conducting any criminal behaviour in these areas. The implementation of CPTED recommendations including clear sight lines, good natural surveillance, natural access control and territorial reinforcement should be achieved to delineate that these car parks are a controlled space and reduce unintentional access. Perimeter security, and vehicle and pedestrian barriers should be used, where appropriate to reduce access opportunities.

Protecting people using the promenade areas require special attention. Use of vehicle(s) as weapons to harm people can be mitigated by using appropriate solution such as Vehicle Security Barriers (fixed, retractable, portable, street furniture, and the like).

Security patrols of the complex should occur to provide deterrence and to respond to security related incidences and lone worker situations.

### 9.6.3 Risk Trend: Theft

#### Threat posed by Theft

		<b>INTENT</b>		
		Little	Expressed	Determined
<b>CAPABILITY</b>	Extensive	Medium	High	Extreme
	Moderate	Low	Significant	High
	Low	Low	Medium	Significant

#### Threat Analysis

Thieves have been assessed as having Expressed Intent, due to the fact that high value goods are likely to be stored within the facility (in particular the cold rooms where the fish stock is stored).

Thieves have been assessed as having Moderate capability due to the ease of access to restricted areas through tailgating, picking locks, break-and-enter, scaling barriers, forced entry etc.

#### Risk Analysis

The risk trend of theft has been assessed as Medium to Low depending on the targeted items.

Markets will have highly valuable goods, cash/cheque deposit safes, highly desirable assets that will need to be secured. Facility assets and property, motor vehicles and items of value stored within motor vehicles may also be targeted.

Security lighting, video surveillance and security signage notifying car park users to not leave valuables in their cars, and that the area is under surveillance will be provided for the car park areas in order to reduce the likelihood of theft from motor vehicles and theft of motor vehicles. These measures if incorporated can reduce the likelihood of items of value being left in vehicles or in plain sight within vehicles, as well as significantly increasing the deterrence aspects and likelihood of detection within the area.

High security mechanical locking system can be incorporated into facility entry points in order to increase the difficulty of unauthorised access into facilities. Electronic access control will be designed to restrict un-authorised access to high risk areas in order to provide an auditing function of access into these areas. This auditing function can also provide deterrence to authorised users of the area from committing theft as they will know the electronic access control system has recorded their access.

An intruder alarm system will be designed to monitor nominated areas within the facility. This system will be able to detect unauthorised access to a monitored area and notify the monitoring location, which can in turn dispatch a suitable response force to apprehend the intruder (if necessary and programmed). Intruder alarm devices such as magnetic reed switches will be designed to monitor the building perimeter, while passive infrared detection devices will be designed to monitor nominated high risk areas.

Contract security guards may be required to patrol the facility, once it's built and operational on an as need basis during busy trading periods where excessive stock is held-on site.

#### 9.6.4 Risk Trend: Antisocial Behaviour

##### Threat posed by Antisocial Behaviour

		<b>INTENT</b>		
		<b>Little</b>	<b>Expressed</b>	<b>Determined</b>
<b>CAPABILITY</b>	<b>Extensive</b>	Medium	High	Extreme
	<b>Moderate</b>	Low	Significant	High
	<b>Low</b>	Low	Medium	Significant

##### Threat Analysis

Antisocial People have been assessed as having Little Intent, as they are more likely to be unplanned offences (due to intoxication, arguments etc.).

Antisocial People have been assessed as having Low capability due to the lack of skills, knowledge and equipment required to conduct this offensive behaviour.

##### Risk Analysis

The risk trend of antisocial behaviour includes harassment, threatening behaviour, public nuisance and drug/alcohol related incidences. These antisocial behaviour risks have been rated as High to Low risks.

Anti-social behaviour, such as loitering and harassment are serious concerns for the staff, vendors, patrons and the general public using the precinct.

While the consequence of these types of risks do not directly impact on the ability for The new Sydney Fish Market to provide their services, it does negatively contribute to the experience of visiting the precinct and reduces the reputation of The new Sydney Fish Market for being a safe and secure destination. Consequently, these risks need to be carefully managed to help ensure that The new Sydney Fish Market owners are seen to do everything possible towards creating a safe environment for the public.

Electronic security measures such as Video Surveillance Systems (VSS), as well as natural surveillance strategies and security lighting can be implemented to deter persons from loitering or conducting anti-social behaviour within the precinct. VSS can also provide recorded video images that may be used for prosecution and conviction purposes of any security incidences. Help Points should be considered for the general public to call for assistance during emergency situations. Fixed duress alarms and mobile duress pendants should be considered for staff working in high risk areas (e.g. cash transaction offices and lone-worker situation).

Regular security guard patrols of the precinct during evenings and night times should be considered, especially around the stock holding areas. The staff of The new Sydney Fish Market should also be aware of response procedures to anti-social behaviour such as loitering or harassment by drug/alcohol affected persons.



### 9.6.5 Risk Trend: Assault

#### Threat posed by Assault

		<b>INTENT</b>		
		<b>Little</b>	<b>Expressed</b>	<b>Determined</b>
<b>CAPABILITY</b>	<b>Extensive</b>	Medium	High	Extreme
	<b>Moderate</b>	Low	Significant	High
	<b>Low</b>	Low	Medium	Significant

#### Threat Analysis

People assaulting staff/contractors/vendors/visitors etc. have been assessed as having Little Intent, as they are more likely to be unplanned offences (due to intoxication, arguments etc.).

People assaulting staff/contractors/vendors/visitors etc. have been assessed as having Low capability due to the lack of skills, knowledge and equipment required to conduct this offensive behaviour.

#### Risk Analysis

The risk trend of assault has been assessed as Low risk based on the likelihood of occurrence.

In order to reduce the likelihood of assault occurring within the precinct, a high importance should be placed on the deterrence and surveillance aspects of the area. Adequate lighting levels, natural surveillance strategies and VSS should be incorporated throughout the precinct including the restaurants, especially around main facility entrances and main thoroughfares throughout the precinct, in order to provide deterrence against committing crimes. VSS is important for post event analysis and to be used for the identification and prosecution of offenders in instances of assault.

Fixed duress alarms should also be provided in high risk areas such as cash transaction office(s) to allow staff call for assistance during emergency situations.

## 9.7 Risk Evaluation

### 9.7.1 General

Evaluating security risk involves determining which risks are tolerable, and which risks require further attention (e.g. treatment).

### 9.7.2 Tolerance of Risk

Decisions on the tolerability of risk for The new Sydney Fish Market has based upon the ALARP approach ('As Low as Reasonably Practical', Figure 6 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.

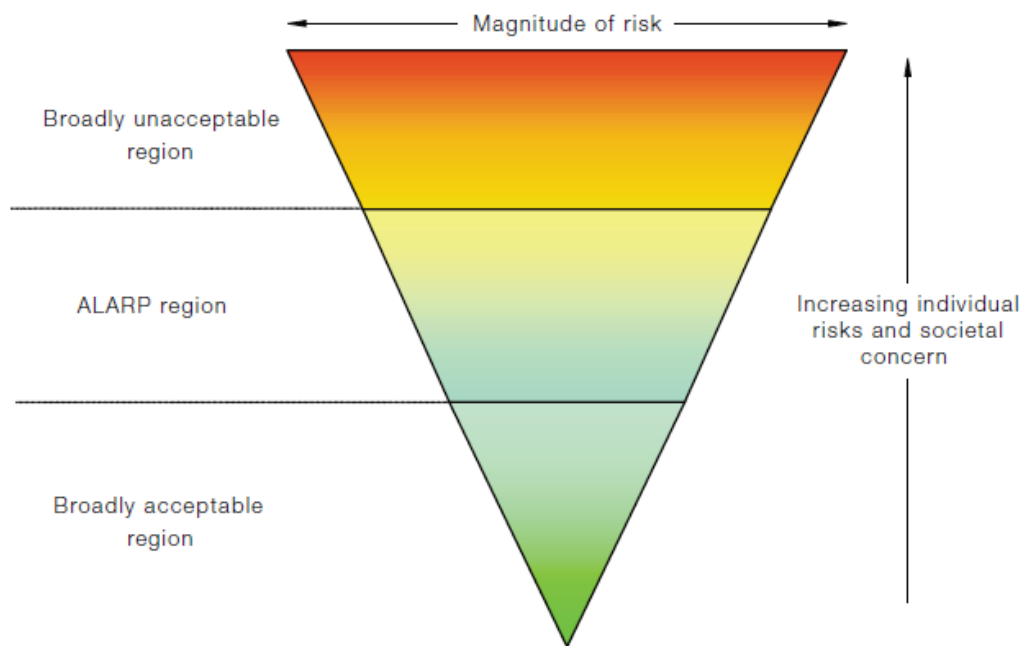


Figure 6 ALARP Approach

#### **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:**

High and Medium risks are required to be reduced as low as reasonably possible. Senior management attention is required for High risks, while management attention is required by Medium risks.

#### **Broadly Acceptable Region:**

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

## **9.8 Risk Treatment**

Risk treatment entails either:

- Avoiding the risk by deciding not to start or continue the activity that causes the risk;
- Taking or increasing the risk in order to pursue an opportunity;
- Removing the risk source altogether;
- Changing the likelihood of the risk;
- Changing the consequences of the risk;
- Sharing the risk with a third party or parties (e.g. Insurance, contracts etc.); and
- Retaining the risk by informed decision.

Refer to Section 10.0 for the risk treatment recommendations.

Refer to Appendix B for the Security Treatment Matrix.

## **9.9 Monitoring & Review**

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 risk management process should be constantly monitored and regularly reviewed to help ensure it remains current, efficient and effective.

The monitor and review step has the objectives of achieving improved:

- Understanding, through:
  - Continuing awareness of changing contexts,
  - Continuing awareness of changing demands,
  - Learning from experience,
  - 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,
  - Enhancing integration with interdependencies; and
- Assurance, through ensuring and confirming compliance with:
  - Strategic requirements,
  - Policy requirements,
  - Operational requirements,
  - 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.

#### 9.9.1 Monitoring & 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 Counterterrorism Unit, 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 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 organisation.

### 9.9.2 Triggering Monitoring & Review Processes

The new Sydney Fish Market should undertake a review of security risk when:

- Significant structural or layout changes are made to the precinct, car park, 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 within the new Sydney Fish Market, increased exposure of events, increase in crime statistics within the LGA);
- The national security threat changes (e.g. the National Terrorism Threat levels);
- Management responsibilities change significantly (e.g. appointment of a new management);
- 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.; and
- Significant new services are provided or the organisation enters new markets.

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, or organisation;
- 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.

### 9.9.3 Post Event Analysis & 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, stakeholders, citizens, etc., where appropriate.

## 10.0 Recommendations

### 10.1 Overview

Identified risks, and in particular the High and Very High risks listed in Appendix A can have their risk ratings reduced to acceptable levels by implementing the risk treatment measure strategies listed in the sections below.

### 10.2 Environment Specific Considerations

The security systems and treatment measures employed at The new Sydney Fish Market will be required to be highly flexible and adaptable in order to provide adequate security to a diverse range of security environment the area is likely to face.

Due to the diverse nature of the business held in the precinct, the security treatment measures will need to provide adequate yet not overbearing security for low risk, low publicity events, while needing to be able to cope with the additional demands required from higher risk, high publicity events.

### 10.3 Site Wide Recommendations

#### 10.3.1 Security Risk Management Policies and Procedures

It is recommended that Security Risk Management Plans, Policies and Procedures be produced in order to help lower the security related risks through operational and procedural controls. These Plans, Policies and Procedures should be developed for The new Sydney Fish Market as a whole including the cooking school, restaurant and bar.

##### 10.3.1.1 Overview

- Prior to The new Sydney Fish Market going operational, it is recommended that The new Sydney Fish Market and or its security operator develop, implement, and maintain a Security Risk Management Process including, but not limited to:
  - A Security Risk Management Policy document;
  - A Security Risk Management Procedure document; and
  - A Security Risk Assessment document.
- A site wide Security Risk Management Process, consisting of the documents listed above is also recommended. The security risk management committee responsible for developing, implementing, and maintaining the site wide Risk Management Process should contain representatives responsible for the security risk management process.
- It is recommended that these documents be produced for the standard day to day operating of the Facility. It is recommended that event specific documents be produced for each new type of event held within the facility, or for each new high profile/high risk event.
- It is recommended that these documents be regularly reviewed and updated as required.

##### 10.3.1.2 Risk Management Process

It is recommended that the facility as a whole develop a security risk management process in order to:

- Identify specific risks to their people, information and assets;
- Identify the acceptable level of risk tolerance for The new Sydney Fish Market Facility;
- Identify appropriate protections to reduce or remove risks; and
- Identify and accept responsibility for untreatable residual risks.

The Security Risk Management Process should ensure that:

- Security risk management is the responsibility of each staff member including contractors, and traders;

- Security risk management, is part of day-to-day business operations;
- The process for managing security risk is logical and systematic, and should form part of the standard management process the facility as a whole; and
- Changes in the threat environment are to be continuously monitored and necessary adjustments made to maintain an acceptable level of risk and a balance between operational needs and security.

The Facility is recommended to adopt a risk management approach to cover all areas of protective security activity across their Facility, in accordance with the International Standard for Risk Management ISO 31000:2009 and the Australian Standard HB 167:2006 Security risk management.

As part of the risk management process, The new Sydney Fish Market is recommended to:

- Establish the scope of any security risk assessment and identify the people, information and assets to be safeguarded;
- Determine the threats to people, information and assets, and assess the likelihood and impact of a threat occurring;
- Assess the risk based on the adequacy of existing safeguards and vulnerabilities; and
- Implement any supplementary protective security measures that will reduce the risk to an acceptable level.

#### **10.3.1.3 Risk Management Policy**

The Risk Management Policy developed, implemented and maintained and the precinct as a whole, is recommended to clearly state the objectives, and commitment to, risk management and typically addresses the following:

- The Facility/Precinct's rationale for managing risk;
- Links between the Facility/Precinct's objectives and policies and the risk management policy;
- Accountability and responsibilities for managing risk;
- The way in which conflicting interests are dealt with;
- Commitment to make the necessary resources available to assist those accountable and responsible for managing risk;
- The way in which risk management performance will be measured and reported; and
- Commitment to review and improve the risk management policy and framework periodically and in response to an event or change in circumstances.

The risk management policy should be communicated appropriately within the Facility/Precinct.

#### **10.3.1.4 Accountability**

The new Sydney Fish Market should strive to ensure that there is accountability, authority and appropriate competence for managing risk, including implementing and maintaining the risk management process and ensuring the adequacy, effectiveness and efficiency of any controls. This can be facilitated by:

- Identifying risk owners that have the accountability and authority to manage risks;
- Identifying who is accountable for the development, implementation and maintenance of the framework for managing risk;
- Identifying other responsibilities of people at all levels in the organisation for the risk management process;
- Establishing performance measurement and external and/or internal reporting and escalation processes; and
- Ensuring appropriate levels of recognition.

### **10.3.2 Security Management, Policies and Procedures**

#### **10.3.2.1 Developing a Security Culture**

To successfully deliver the Security Management Plan, Policy and Procedures, The new Sydney Fish Market need to foster a professional culture and a positive attitude towards protective security.

It is recommended that The new Sydney Fish Market provide all staff, including contractors, vendors and tenants with sufficient information and security awareness training to ensure they are aware of, and meet the requirements of the Security Management Plan, Policy and Procedures for the Facility at which they are employed.

It is recommended that The new Sydney Fish Market should consider the following:

- Ensure that individuals who have specific security duties receive appropriate, up to date training;
- Have an ongoing security awareness program to inform and regularly remind individuals of security responsibilities, issues and concerns;
- Communicate and make available to all staff, including contractors, vendors their protective security policies, plans and procedures.

To fulfil their security obligations, it is recommended that The new Sydney Fish Market appoint:

- A person responsible for the facility protective security policy and oversight of protective security practices;
- A person responsible for the day-to-day performance of protective security functions; and
- A person responsible for the security of the Facility's Information Communications Technology (ICT) systems.

These appointed personnel are recommended to have detailed knowledge of facility specific protective security policy, protocols and mandatory protective security requirements in order to fulfil their protective security responsibilities.

#### **10.3.2.2 Security Policies and Procedures**

It is recommended that The new Sydney Fish Market and tenants develops their own set of protective security policies and procedures to meet their specific business needs.

The policy and procedures are recommended to:

- Detail the objectives, scope and approach to the management of protective security issues and risks within the Facility;
- Be endorsed by senior management;
- Identify protective security roles and responsibilities;
- Be reviewed and evaluated in line with changes to Facility business and security risks;
- Be consistent with the Facility's security risk assessment findings;
- Explain the consequences for breaching the policy or circumventing any associated protective security measure; and
- Be communicated on an ongoing basis and be accessible to all Facility employees, and where reasonable and practical be publicly available.

### **10.3.3 Business Continuity Management**

#### **10.3.3.1 Business Continuity Overview**

It is recommended that Business Continuity Management Plans and Procedures be produced in order to help lower the security business operations related risks associated with emergency/crisis situations.



### 10.3.3.2 Business Continuity Management

Critical services and associated assets need to remain available in order to assure the health, safety, security and economic well-being of the contractors, and visitors.

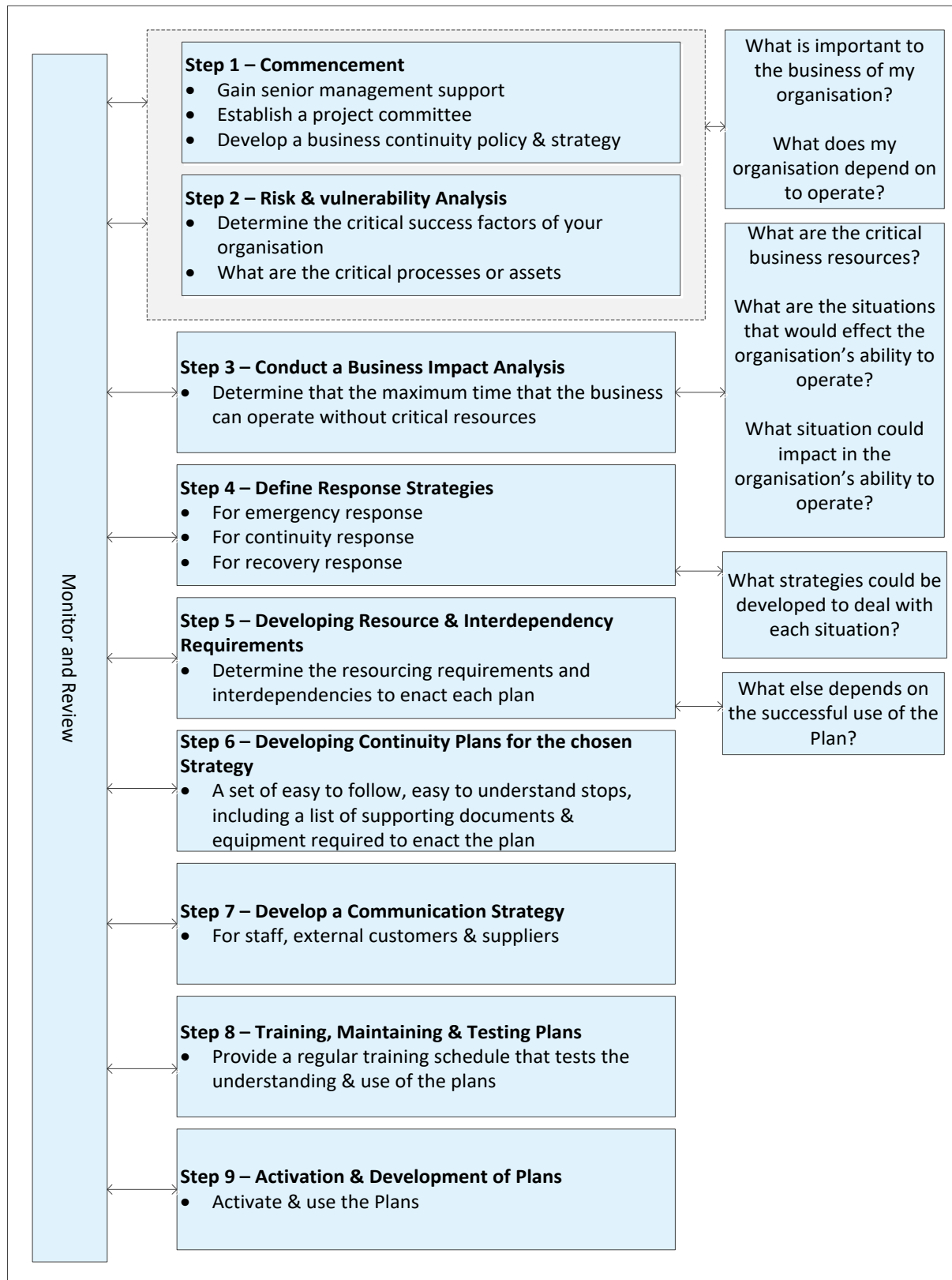
Business continuity management (BCM) is recommended to be implemented as part of the facility overall approach to effective risk management. BCM is the process The new Sydney Fish Market and its tenants to follow in the event of a disruption to business. A key risk for The new Sydney Fish Market is that they will be unable to remain operational in the event of a crisis and/or disruption.

It is recommended that The new Sydney Fish Market establish a business continuity management program to provide for the continued availability of critical services and assets, and of other services and assets when warranted by a threat and risk assessment.

It is recommended to:

- Develop a governance structure establishing authorities and responsibilities for a BCM program, and for the development and approval of business continuity plans;
- Within the context of the identification of assets, undertake impact analysis to identify and prioritise the Facility's critical services and assets, including identifying and prioritising information exchanges provided by, or to other Facilities, or other external parties and tenants;
- Undertake activities to monitor the Facility's level of overall preparedness; and
- Make provision for the continuous review, testing and audit of business continuity plans.

Facilities are recommended to follow the Business Continuity Management process outlined in Figure 7 below;



**Figure 7 Business Continuity Management Process**

### **10.3.4 Emergency Management**

#### **10.3.4.1 Overview**

It is recommended that Emergency Management Plans and Procedures be produced in order to help lower the security related risks associated with emergency situations.

#### **10.3.4.2 Emergency Management Plan**

It is recommended that an Emergency Planning Committee (EPC) be established at The new Sydney Fish Market, to provide a coordinated emergency management plan for emergencies that affect the whole complex including tenants.

It is recommended that The new Sydney Fish Market EPC consist of representatives from vendors, major contractors and tenants.

It is recommended that the EPC's develop an Emergency Management Plan for The new Sydney Fish Market as a whole.

It is recommended that the emergency management plan includes, but not be limited to, the following key elements:

- A clear statement of purpose and scope;
- Information on the structure and purpose of the EPC;
- Identification of the facilities to which it applies;
- Descriptions of the fire safety and emergency features of the facility;
- The organisational arrangements for the facility;
- Separate sections for the following:
  - The emergency identification outcomes;
  - The emergency response procedures;
  - The evacuation diagram;
  - Training arrangements;
- A statement of the extent of distribution of the emergency plan or excerpts from the emergency plan;
- A record of distribution, including where personal emergency evacuation plans (PEEPs) for people with disabilities are held. For example PEEPs should be held by the relevant warden;
- Details of the hours of occupancy of the facility;
- The EPC nominated validity period for the emergency plan; and
- The date of issue or amendment date on each page of the emergency plan.

If an electronic format is used for the emergency plan, it is recommended that at least one printed copy be available on site.

#### **10.3.4.3 Emergency Response Procedure**

##### **10.3.4.3.1 General**

It is recommended that the new Sydney Fish Market and the security operator develop an Emergency Response Procedure.

An emergency response procedure should be developed for whole of site addressing the following:

- Responsibilities, duties and the actions by key emergency responders to take during an emergency;
- The responsibilities of facility occupants and the actions they are to take in an emergency;
- The arrangements for evacuating the facility;

- The arrangements for emergency preparedness and response; and
- The current emergency contact details.

The specific information included in the emergency response procedures should be determined by the EPC in collaboration with the facility owners, managers, occupiers and employers. The EPC should also determine any other information that is to be included, as appropriate to each specific Facility.

#### **10.3.4.3.2 After-Hours Procedures**

The specific needs of people who may be present outside the normal hours of business/operation should be considered.

#### **10.3.4.3.3 Communication**

The emergency procedures should address the method of warning and communication to be used during an emergency.

The needs of occupants and visitors with a disability should be considered when developing procedures for emergency warning. This may entail alternative means of communicating emergency information and warnings.

Consideration should be given to communications with neighbouring facilities.

#### **10.3.4.3.4 Communications Equipment**

For continuity of communications in an emergency, consideration shall be given to the following:

- The utilisation of multi-modal communication systems for emergency responses. NOTE: Multi-modal communication systems are intended to ensure continuity of communication in the event of the failure of the primary communication system. Examples are:
  - EWIS;
  - Visual and tactile signals;
  - Telephones (including mobile telephones);
  - Two-way radio;
  - Paging systems; and
  - Public address systems.
- The limitations of transmitting equipment technology in certain types of emergencies.
- The potential effects of using equipment producing electromagnetic radiation in situations where such signals could have adverse effects on explosive devices or essential equipment, such as sensitive medical equipment, that may be in the same location. NOTE: Equipment producing electromagnetic radiation includes mobile phones, radio sets and appliances using wireless technology transmission.
- Any battery-powered equipment that needs fully charged batteries available.
- The potential failure of equipment that is mains-powered without battery backup.

#### **10.3.4.3.5 Control and Coordination**

The procedures should identify an appropriate location from which the chief warden can establish control, communication and coordination, and liaise with the Emergency Services.

An alternative location(s) are recommended to be nominated in the emergency response procedures to allow for contingencies.

#### **10.3.4.3.6 Emergency Response Equipment**

The procedures should include appropriate information and instructions on the use of any emergency response equipment that is in place in a facility.

Emergency response equipment is recommended to include, but not be limited to fire extinguishers, fire hose reels, first aid kits, spill clean-up kits, breathing apparatus and the like.

#### 10.3.4.3.7 Evacuation:

##### General

The emergency response procedures should address the actions that are to be taken to evacuate the Facility by members of the ECO, occupants and visitors.

As appropriate to the Facility, the emergency response procedures should include requirements that the ECO members:

- Check their area of responsibility to determine whether all persons have been evacuated; and
- Report the result of the check to the chief warden, including whether any refuge is occupied.

This function is of greater importance than a later physical count of those evacuated.

##### Occupants and Visitors with a Disability

The evacuation arrangements for persons with a disability should be considered in the development of the emergency response procedures.

##### Evacuation Options

The procedures should address the extent of evacuation from a Facility that is necessary for different types of emergencies. Consideration should be given to the following evacuation options, as appropriate to the Facility:

- Full evacuation - This measure is used to clear the Facility of all occupants; and
- Partial evacuation - This measure is an alternative to a total evacuation.

Partial evacuation may:

- Include evacuation into or through smoke and fire compartments;
- Be used to evacuate individuals closest to a situation and to prevent congestion in the stairways; or
- Be utilised when evacuation of several floors is sufficient to protect occupants while the hazard is being eliminated, i.e., to move people away from a localised emergency within the Facility
- Shelter in place (no evacuation) - This measure is an emergency response option that allows occupants and visitors to remain inside the Facility on the basis that an evacuation to an external-to-building location might reasonably expose evacuated people to a greater level of danger.

An assessment of the shelter or refuge to determine the suitability and sustainability of the shelter should be carried out for certain emergencies, where shelter in place option is being considered.

The success of this strategy will depend, to a large extent, on the degree to which premises have been prepared. The most appropriate decision will be made after the assessment of all the available information. Decision-makers should seek and evaluate expert advice.

#### **NOTES:**

- Full evacuation would normally be carried out in response to a potentially catastrophic, life threatening situation or where the Facility cannot function due to a severe services malfunction.
- In some buildings, the alarm system is automatically set to the evacuate tone without utilising an alert tone facility. Emergency response procedures should reflect these situations.
- Examples of where a partial building evacuation may be carried out include a localised fire, a localised flood, a chemical spill, or a bomb threat specified for a certain area.
- Numerous situations can occur that make it advisable for those inside a building to remain inside for their own protection. These procedures may be warranted if, for example, a protest/demonstration that is taking place outside the building turns violent.

### Evacuation Routes

The likely effect that a particular emergency may have on evacuation routes and normal paths for leaving the facility is recommend to be considered.

### Assembly Areas

Assembly areas should, so far as is reasonably practicable, be sufficiently distant from the emergency for the protection of evacuees.

#### **NOTES:**

- Ideally the areas selected should be sheltered from the affected Facility and should allow for further movement away from the emergency. Consideration should be given to dangers such as smoke and flying/falling debris and other objects.
- An assembly area should be accessible by a route suitable for people who walk with difficulty or use mobility aids, including walking frames and wheelchairs, and prams.
- The movement of large numbers of people has its inherent dangers, particularly in heavy traffic. Careful thought should be given to determine the safest routes from the facility to the nominated places of assembly, including alternatives, and to ensure access for emergency vehicles is not hindered.
- Evacuation may be to another nominated internal or external area, such as another floor or refuge.
- Alternative assembly area(s) may be necessary if the nominated assembly area is unsuitable.

### External Sources:

The characteristics of, and hazards from, external sources should be considered.

### First Aid Officers:

Where first aid officers exist, their duties during an emergency should be considered by the EPC.

The roles of the first aid officers and wardens should be separate and distinct.

### Lifts and Escalators:

Lifts and escalators should not be relied upon as a means of evacuation from fire unless their suitability for that purpose has been nominated through a regulatory approval process.

NOTE: Lifts and escalators may be appropriate for use in other types of emergencies and in some circumstances, particularly in emergencies other than fire.

### Media Response:

Restrictions should be placed on contacting print or electronic media during the emergency.

All media statements should be provided, released and authorised by nominated persons ONLY.

### Occupants and Visitors with a Disability:

When developing emergency response procedures, consideration should be given to occupants and visitors who for one reason or another may need assistance or are unlikely to be able to act optimally in an emergency. This would include but not be limited to occupants and visitors who:

- Are accompanied by an assistant;
- Have a guide or companion animal;
- Use alternative forms of information and communication;
- Have an ambulatory disability;
- Use a wheeled mobility appliance, including wheelchair or scooter;
- Are easily fatigued;

- Easily experience acute anxiety in an emergency; or
- Easily experience extreme confusion in an emergency.

A current list of the names, workplaces and other necessary information about occupants with a disability should be kept at the locations where the chief warden exercises control.

Suitable strategies in an emergency or evacuation should be discussed with those occupants from the Facility who have a disability and a personal emergency evacuation plan (PEEP) developed for each of those persons.

Information on the PEEP should be disseminated to all people responsible for its implementation.

Organisation of the Facility:

The organisational arrangements for the new Sydney Fish Market should be considered. This includes the human resources aspects of the new Sydney Fish Market.

People Unfamiliar with the Emergency Response Procedures:

The needs of people who may be within a facility and are not familiar with the emergency response procedures shall be considered.

Personal Effects:

When being evacuated, occupants and visitors may be asked to take their immediately available personal effects such as handbags, wallets and car keys if it is safe to do so.

Refuges:

Refuges should be considered where practical.

Refuges are areas where occupants and visitors may wait for their delayed independent evacuation, or assisted evacuation by Emergency Services or other nominated personnel.

NOTE: Refuges are normally nominated by the relevant certifier.

Occupants who have a disability should be attended in the refuge by another person.

Specialist Staff:

The roles of security guards, receptionists and other specialist staff shall be considered.

Stairway Evacuation Device:

Consideration should be given to the use and suitability and storage arrangements of stairway evacuation devices for people who use wheelchairs or who otherwise would need to be carried down the stairway.

NOTE: Any stairway evacuation device should be operated by a competent person.

Vehicle Entry Points:

Consideration should be given to imposing restrictions on vehicular movement during an emergency.

**NOTES:**

Persons should be nominated by the chief warden to restrict vehicle movements into/around the Facility.

Persons should be nominated by the chief warden to be at entry points to the Facility to meet responding Emergency Service(s).

### **10.3.5 Information Security**

#### **10.3.5.1 General**

It is recommended that Information Security treatment measures be implemented, where appropriate in order to help lower the security related risks associated with precinct information and information assets.

#### **10.3.5.2 Overview**

It is recommended that The new Sydney Fish Market develop, document, implement and review appropriate security measures to protect their information from unauthorised use or accidental modification, loss or release by:

- Establishing an appropriate information security culture within the precinct;
- Implementing security measures that match the information's value, classification and sensitivity; and
- Adhering to all legal requirements.

The information security policy is recommended to be developed based on the following three elements of information security:

- Confidentiality: ensuring that information is accessible only to those authorised to have access;
- Integrity: safeguarding the accuracy and completeness of information and processing methods, and
- Availability: ensuring that authorised users have access to information and associated assets when required.

Information assets requiring protection should include any form of information, including:

- Electronic data;
- The software or information and communication technology (ICT) systems and networks on which the information is stored, processed or communicated;
- Printed documents and papers;
- The intellectual information (knowledge) acquired by individuals; and
- Physical items from which information regarding design, components or use could be derived.

#### **10.3.5.3 Information Security Policy and Planning**

The new Sydney Fish Market are recommended to provide clear direction on information security through the development and implementation of a precinct information security policy, and address precinct information security requirements as part of the security plan.

The policy and plan are recommended to:

- Detail the objectives, scope and approach to the management of information security issues and risks within the precinct;
- Be endorsed by The new Sydney Fish Market Management;
- Identify information security roles and responsibilities;
- Detail the types of information that an employee:
  - Can lawfully disclose in the performance of his or her duties, or
  - Must obtain authority to disclose,
- Be reviewed and evaluated in line with changes to precinct business and information security risks;



- Be consistent with the requirements of the precinct's protective security plan and information security risk assessment findings;
- Address the issue of data aggregation;
- Include details of the precinct's declassification program;
- Explain the consequences for breaching the policy or circumventing any associated protective security measure, and
- Be communicated on an on-going basis and be accessible to all precinct employees, and where reasonable and practical be publicly available.

#### **10.3.5.4 Information Security Framework**

The new Sydney Fish Market is recommended to establish an information security framework to provide direction and coordinated management of information security for the site. Frameworks should be appropriate to the level of security risks to the precinct's information environment.

The new Sydney Fish Market are recommended to:

- Document requirements for information security when entering into outsourcing contracts and arrangements with contractors and consultants;
- Enter into memorandums of understanding (MOU) with tenants or organisations when regularly sharing information;
- Ensure that prior to providing third parties access to precinct information and ICT systems, security measures that match the security classification or dissemination limiting marker of the information or ICT system are in place, or clearly defined, in appropriate agreements or contracts; and
- Ensure that appropriate permissions are received before providing third parties access to information not originating within the precinct.

#### **10.3.5.5 Information Asset Classification and Control**

The new Sydney Fish Market are recommended to implement policies and procedures for the security classification and protective control of information assets (in electronic and paper-based formats) which match their value, importance and sensitivity. It is recommended that:

- All major information assets including hardware, software and services used in precinct operations (including physical information assets used to process, store or transmit information) are identified, documented and assigned owners for the maintenance of security measures;
- The classification of all precinct information is in accordance with the classification system implemented at the new Sydney Fish Market;
- The control of all security classified information (including handling, storage, transmission, transportation and disposal) is in accordance with the established information security protocols and procedures;
- Information is appropriately marked, stored and handled in accordance with the precinct information security procedures;
- A classification guide specific to the precinct is developed, maintained and accessible to all precinct employees;
- The precinct classification guide does not limit the provisions of relevant legislative requirements or international obligations under which the precinct operates; and
- Disposal of information records is in accordance with legislative and regulatory requirements.

#### **10.3.5.6 Operational Information Security Management**

The new Sydney Fish Market are recommended to document and implement operational procedures and measures to ensure information, ICT systems and network tasks are managed securely and consistently, in accordance with the level of required security.

Facilities are recommended to ensure, where practical that they:

- Put in place incident management procedures and mechanisms to review violations and to ensure appropriate responses in the event of security incidents, breaches or failures;
- Put in place adequate controls to prevent, detect, remove and report attacks of malicious and mobile code on ICT systems and networks;
- Put in place comprehensive systems maintenance processes and procedures including operator and audit/fault logs and information backup procedures;
- Implement operational change control procedures to ensure that they appropriately approve and manage changes to information processing facilities or ICT systems;
- Comply with legal requirements when exchanging information in all forms, between Facilities and/or third parties;
- Apply the classification schemes and measures defined in the precinct Information Security Plans, Policies and Procedures;
- Comply with the precinct Information Security Plans, Policies and Procedures when exchanging information in all forms, between Facilities and/or third parties, and
- Comply with e-commerce legal requirements for on-line transactions and services.

#### **10.3.5.7 Information Access Controls**

The new Sydney Fish Market are recommended to have in place control measures based on precinct requirements and assessed/accepted risks for controlling access to all information, ICT systems, networks (including remote access), infrastructures and applications. The precinct access control rules should be consistent with individual business requirements and information classification as well as legal obligations.

Facilities are recommended to ensure, where practical that they:

- Require specific authorisation to access ICT systems;
- Assign each user a unique personal identification code and secure means of authentication;
- Define, document and implement policies and procedures to manage operating systems security, including user registration, authentication management, access rights and privileges to ICT systems or application utilities;
- Display restricted access and authorised use only (or equivalent) warnings upon access to ICT systems;
- Where wireless communications are used, appropriately configure the security features of the product to at least the equivalent level of security of wired communications;
- Implement control measures to detect and regularly log, monitor and review ICT systems and network access and use, including all significant security relevant events;
- Conduct risk assessments and define policies and processes for mobile technologies; and
- Assess security risks and implement appropriate controls associated with use of ICT facilities and devices (including The new Sydney Fish Market issued equipment) such as mobile telephony, tablets, laptops, personal storage devices and internet and email prior to connection.

#### **10.3.5.8 Information System Development and Maintenance**

The new Sydney Fish Market are recommended to have in place security measures during all stages of ICT system development, as well as when new ICT systems are implemented into the operational environment. Such measures must match the assessed security risk of the information holdings contained within, or passing across, ICT networks infrastructures and applications.

When establishing new ICT systems or implementing improvements to current ICT systems including off-the-shelf or outsourced software development, Facilities are recommended to ensure that they:

- Address security during the early phases of the systems development life cycle, including the system concept development and planning phases and then in the requirements analysis and design phases;
- Consult internal and/or external auditors when implementing new or significant changes to financial and critical business ICT systems;
- Incorporate processes including data validity checks, audit trails and activity logging in applications to ensure the accuracy and integrity of data captured or held in applications;
- Carry out appropriate change control, acceptance and ICT system testing, planning and migration control measures when upgrading or installing software in the operational environment;
- Control access to ICT system files to ensure integrity of the systems, applications and data; and
- Identify and implement access controls including access restrictions and segregation/isolation of ICT systems into all infrastructures, business and user developed applications.

#### **10.3.5.9 Compliance**

The new Sydney Fish Market are recommended to ensure that information security measures for all information processes, ICT systems and infrastructure adhere to any legislative or regulatory obligations under which the Facility operates.

To ensure all legal, statutory, regulatory, contract or privacy obligations relating to information security are managed appropriately, The new Sydney Fish Market are recommended to:

- Take all reasonable steps to monitor, review and audit information security effectiveness, including assigning appropriate security roles and engaging internal and/or external auditors and specialist organisations where required; and
- Regularly review all information security policies, processes and requirements including contracts with third parties, for compliance and report to management.

### **10.3.6 Physical Security Measures**

#### **10.3.6.1 General**

It is recommended that physical security treatment measures be implemented where appropriate in order to help lower the security risk profile of The new Sydney Fish Market precinct.

#### **10.3.6.2 Physical Security Policy and Planning**

It is recommended that The new Sydney Fish Market provide clear direction on physical security through the development and implementation of Precinct Physical Security Policy, and address physical security requirements as part of The new Sydney Fish Market Security Plan.

The policy and plan are recommended to:

- Detail the objectives, scope and approach to the management of physical security issues and risks within the precinct;
- Be endorsed by the Facility's senior management;
- Identify physical security roles and responsibilities;
- Continuously review physical security measures to reflect changes in the threat environment and take advantage of new cost effective technologies;
- Be consistent with the requirements of The new Sydney Fish Market protective security plan and physical security risk assessment findings;
- Explain the consequences for breaching the policy or circumventing any associated protective security measures; and
- Be communicated on an ongoing basis and be accessible to all The new Sydney Fish Market employees.

### 10.3.6.3 Physical Security Measures

- Provide suitable vehicle and pedestrian gates and calming devices at appropriate locations. Car parks and loading docks in particular will require vehicular security devices such as security gates and boom gates.
- Provide high security locking devices, and well-constructed doors, door frames and door hardware to restrict forced entry attempts.
- Provide vehicle safety barriers (bollards, street furniture and the like) to restrict unauthorised vehicle access and to mitigate any hostile vehicle attacks.

### 10.3.7 Electronic Security Measures

#### 10.3.7.1 General

It is recommended that electronic security treatment measures be implemented where appropriate in order to help lower the security risk profile of The new Sydney Fish Market.

#### 10.3.7.2 Electronic Security Measures

It is recommended that the following electronic security measures are provided to The new Sydney Fish Market where practical:

- Provide electronic access control to control access from public to restricted areas, and to provide an auditing function. Electronic access control should be placed in higher risk restricted areas, where the auditing function would be beneficial and also high use areas where the electronic access control would be more beneficial than lock and key mechanical systems.
- Provide an intruder alarm system to monitor nominated restricted areas during non-operational hours. Passive infrared detection devices should be used to monitor the integrity of high risk areas, while magnetic reed switches should be used to monitor nominated perimeter and internal doors.
- Provide CCTV to provide deterrence, surveillance and incidence capturing capabilities.
- Electronic security systems would need to be connected to nominated monitoring locations.
- Help point systems to be provided to allow the public to call for assistance during emergency situations.
- Duress alarm system to be provided in high risk staff areas such as cash transaction offices to allow staff to call for assistance during emergency situations.

### 10.3.8 Personnel Security Measures

#### 10.3.8.1 Overview

It is recommended that personnel security treatment measures be implemented where appropriate in order to help lower the security risk profile of The new Sydney Fish Market precinct.

#### 10.3.8.2 Security Awareness Training

Security awareness training is an important element of protective security. Awareness training supports physical, information and personnel security measures as well as informing staff of their governance requirements.

To truly change staff behaviours, a security awareness campaign should effectively communicate what is enforced (Facility policies) and in addition communicates why, then follows up the campaign with strong, visible enforcement, and rewards.

Employees should undertake security awareness as soon as possible after starting. It is recommended that security awareness training is included as part of the induction programs.

The new Sydney Fish Market are recommended to hold regular refresher training sessions to confirm prior knowledge and inform employees of any new measures. It is also recommended to conduct additional training if the threat environment changes.

The new Sydney Fish Market can develop security awareness through:

- Campaigns that address the ongoing needs of the precinct and the specific needs of sensitive areas, activities or periods of time;
- Security instructions and reminders via publications, electronic bulletins and visual displays such as posters;
- Protective security related questions in staff selection interviews;
- Drills and exercises; and
- Inclusion of security attitudes and performance in the precinct performance management program.

It is recommended that The new Sydney Fish Market provide security awareness training/briefings to their employees and any contractors based in at the precinct. It is recommended that this training be provided initially as part of the employee induction process or as soon as possible after commencement.

It is recommended that The new Sydney Fish Market provide targeted security awareness training when the precinct has an increased or changed threat environment.

Further, Security awareness training should cover the following areas as minimum:

- Security procedures and policies;
- Personal safety measures;
- Asset protection;
- Protection of official information from:
  - Inappropriate use;
  - Loss; and
  - Corruption;
- Reporting requirements including:
  - Changes of circumstances; and
  - Incident reporting;
- Additional security briefings.

#### **10.3.8.3 Internal Reporting Contacts**

It is recommended that The new Sydney Fish Market provide employees with a list of key reporting contacts. The contacts list should cover, but is not limited to, how to report:

- Suspicious behaviour;
- Threatening behaviour including letters, bomb threats and phone calls;
- Broken ICT and security equipment;
- Security infringements and breaches;
- Fraud or suspected fraud;
- Full secure waste bins; and
- Lost access cards.

#### **10.3.8.4 Contract/In-House Security Guards**

It is recommended that an appropriate number of security guards be provided for busy trading periods. The new Sydney Fish Market are recommended to determine the number of guards required based on the specific risk profile, tasks to be performed.

It is recommended that security guards be provided to perform a roaming patrol of the Public Realm during peak trading hours.

It is recommended that security guards perform their duties in line with AS 4421 Guards and Patrol Security Services.

#### *Security Contractors Assignment Instructions*

It is recommended that the contract between The new Sydney Fish Market and the Contract Security Provider (or in-house) include an assignment of instructions for all relevant duties associated with the guarding operation(s). The following details shall be included in the assignment instructions:

- The location and details of site(s) or valuables to be protected, with name(s) of relevant contacts provided by The new Sydney Fish Market and the agreed means of site access;
- The location of, and relevant operator(s) at, the Facility's operations room;
- The number of personnel involved in the assignment and their responsibilities with particular respect to the following:
  - Patrol routes and routine reporting points and times;
  - Working hours and handover requirements;
  - Emergency procedures;
  - Communication procedures;
  - Specifically requested services;
  - Access control and searching procedures;
  - Facilities, vehicles or equipment; and
- The accountability for, and any restrictions concerning, individual actions.

## **10.4 Public Realm**

### **10.4.1 Passive Security Measures (CPTED)**

It is recommended that Crime Prevention through Environmental Design principles to be applied to the detailed design of the Public Realm to passively help lower the risk profile of the Public Realm areas. It is recommended that CPTED principles be incorporated through:

- clearly delineate public areas from restricted areas;
- maintain clear sightlines throughout the precinct;
- external lighting designs which provides appropriate and uniform lighting that promotes passive and active surveillance. In particular, main facility entrances and the main thoroughfares throughout the precinct including the pedestrian walkways;
- utilising, where practical surfaces and finishes that facilitate the rapid repair of vandalism and removal of graffiti, and reduce the likelihood for vandalism/graffiti;
- providing security and way-finding signage where appropriate to help delineate between public and private space, control pedestrian and vehicular movement throughout the Precinct, and to provide deterrence against criminal or anti-social behaviour;
- keeping vegetation in and around the sites, and throughout the precinct appropriately maintained and to a low height in order to more easily facilitate natural and active surveillance throughout the area.

### **10.4.2 Vegetation Maintenance Strategy**

It is recommended that following a maintenance strategy such as the one depicted below for the Public Realm vegetation will help enhance the CPTED aspects of the precinct;

#### 10.4.2.1 Grassed Areas

- Edges are neat and in trimmed condition.
- Lawns are damage free and have an even surface appropriate for its relevant use.
- Free from lifting of turf.
- Edge of any borders are neat and to a length appropriate for its function.
- Line markings are legible.

#### 10.4.2.2 Garden Beds

- Maintained to appropriate size.
- There are no damages stems, branches, bark or foliage.
- Uniform covering of mulch (where required).
- Where adjacent to windows, ensure height of growth is below the sill height.

#### 10.4.2.3 Trees and Shrubs

- Growth should not adversely affect the ground or building elements with no trip hazard from roots.
- No damage to stems, branches, bark or foliage of trees and shrubs.
- Trimmed so as to minimise the risk of fire, interference of natural light, obstruction of security and to maintain healthy growth.
- Shrub growth to be kept within garden beds and below sill height where adjacent to windows.
- Trees and shrubs must not obstruct signage or other way finding fixtures.

### 10.4.3 Electronic Security Measures

#### 10.4.3.1 Video Surveillance System (VSS)

Video surveillance for the Public Realm is recommended, in order to provide deterrence, monitoring and evidence capturing capabilities.

It is recommended that the majority of CCTV cameras provided throughout the Public Realm area be combination of fixed and PTZ type cameras to allow the Security Guards increased functionality to follow and monitor individuals/areas of interest.

Megapixel cameras, with good low light level performance, and wide dynamic range performance will be provided throughout Public Realm areas in order to achieve appropriate video image quality.

Camera housings which are IP66 rated, vandal resistant will be specified.

Public Realm CCTV cameras are to be monitored from the Security Control Room.

#### 10.4.3.2 Emergency Help Points

An emergency Help Point system is recommended to be provided within the Public Realm to allow members of the public to contact the security control room centre during emergency situations.

Help Points are recommended to be integrated with the CCTV System, so that when a Help Point is activated the images from nearby CCTV cameras are automatically displayed on the Operator Workstations.

Help Point Units will enable direct communication between the Help Point user and Security Control Room operator.

### 10.4.4 Physical Security Measures

It is recommended that the following physical security measures be provided within the Public Realm where practical in order to physically control and restrict access:

- Vehicle barriers (to meet PAS 68/IWA 14-1 standards in selected locations);

- Gates;
- Fencing; and
- Bollards (to meet PAS 68/IWA 14-1 standards in selected locations).

## **10.5 Conclusion**

If implemented, the risk treatment measure strategies listed in the preceding sections above, and in Appendix B can help reduce the risk profile for the precinct. These recommendations will be used to help guide the detailed security services designs during the Design Phases of the Project.



## About AECOM

AECOM is built to deliver a better world.

We design, build, finance and operate infrastructure assets for governments, businesses and organisations in more than 150 countries. As a fully integrated firm, we connect knowledge and experience across our global network of experts to help clients solve their most complex challenges.

From high-performance buildings and infrastructure, to resilient communities and environments, to stable and secure nations, our work is transformative, differentiated and vital. A Fortune 500 firm, AECOM had revenue of approximately \$17.4 billion during fiscal year 2016.

See how we deliver what others can only imagine at [aecom.com](http://aecom.com) and [@AECOM](https://twitter.com/AECOM).

# Appendix A

## Security Risk Matrix

## Security Risk - Treatment Register

#	Key Identified Risks	Treatment	Action By
1	Facility Location & Exposure	Due to the location, profile and media exposure of NFM, a flexible and scalable security solution will need to be provided in order to adequately treat the diverse range of risks the Precinct is likely to be exposed to. The following Precinct wide treatment measures should be provided;	NFM/Operator
		Installation of appropriate Precinct lighting to ensure CCTV has clear view of any activity within the Public Realm, and to assist natural surveillance.	NFM/Operator
		Installation of Precinct CCTV Cameras to provide general surveillance of the Precinct, and to provide deterrence to antisocial/criminal behaviour. An emergency help point system should be considered within the Public Realm to allow members of the public to contact the Security Control Room in emergency situations. Mobile security guards should be provided to perform a roaming patrol of the Precinct and to provide a response to security situations. The number of mobile security guards to be determined based on the risk profile of the current events being held within the Precinct at that point in time.	NFM/Operator
		Crime prevention through environmental design (CPTED) principals should be incorporated into the Precinct layout and landscaping. The Precinct design should enhance natural surveillance by providing clear sight lines and eliminating areas of concealment, provide natural access control and promote territorial reinforcement.	NFM/Operator
2	Unauthorised Access - Pedestrian	Implementation of appropriate staff identification cards and electronic access control to the Facilities/Precent, and to sensitive or key areas within each Facility. Physical security measures to control access into and throughout the Precinct and Facilities. Creation of check points during events to restrict unauthorised access into Precinct/Facilities/areas within facilities. Provision of intrusion detection system to monitor key areas of facilities and to detect unauthorised access to these areas. On site security to provide a timely and appropriate response to unauthorised access.	NFM/Operator
3	Unauthorised Access - Vehicle	For high risk, high profile events where high profile dignitaries etc will be present NFM security will be required to liaise with and coordinate security requirements with relevant security organisations (eg NSW Police, AFP representatives).	NFM/Operator
		During high risk events, additional vehicle access control mechanisms, such as vehicle check points should be created where credentials and other bona fides are assessed prior to gaining entry to the site/next check point. Higher risk events should implement a 'Defence in Depth' approach to perimeter security consisting of concentric layers of security barriers with check points at each barrier.	NFM/Operator
		As part of the permanent security provisions for NFM, an appropriate security gate/entry barrier/boom gates should be provided in nominated locations to deter and delay unauthorised vehicles from accessing the site. These devices should be used in conjunction with other vehicular control devices such as perimeter fences, curbing, bollards and natural access control (CPTED) strategies. Intercoms with remote door release functionality and electronic access control should also be provided at the security gate/entry barrier to allow authorised access.	NFM/Operator
		Ensure that the only vehicles required on site are those of making deliveries and NFM vehicles, which will enable a clearer and swifter identification of unauthorised vehicles. This vehicular control strategy will involve staff and the general public only being able to access the public car park.	NFM/Operator
		As the NFM Precent is largely an open design, boom gates/gates will predominantly be installed at car park entry/exit points, and the entry/exit points to loading docks and the secure service yard.	NFM/Operator

#	Key Identified Risks	Treatment	Action By
4	Forced Access - Pedestrian	Physical and electronic access control measures to be provided to restrict unauthorised access to Precinct/Facilities. Intruder detection system (PIR's/Reed Switches) to be provided to monitor the integrity of nominated locations, and to notify the Security Control Room of a breach.	NFM/Operator
5	Forced Access - Vehicle	Portable anti-ram vehicle barriers may be required for specific high risk events based on the events' risk profile.	NFM/Operator
6	Unauthorised Access - Waterborne	Sydney Harbour Foreshore Authority and the Water Police will need to be liaised and coordinated with in order to provide monitoring and restricted zones in the Harbour. The Harbour itself provides a level of natural access control. Lighting and CCTV will be required along the Harbour side of the Precinct to improve surveillance of this area and deter intruders. Integrated signage to depict restricted access to the Wharf terminals should be considered.	NFM/Operator
7	Mechanical failure of security equipment	Implement a regular maintenance regime, redundancies and system back ups/spare equipment to be provided in accordance with Australian standards and industry best practice. Contractors responsible for repair/replacement of failed equipment to be contracted to repair/replace equipment within nominated timeframes.	NFM/Operator
8	Mechanical failure critical building services/equipment	Implement a regular maintenance regime, redundancies and system back ups/spare equipment to be provided in accordance with Australian standards and industry best practice. Contractors responsible for repair/replacement of failed equipment to be contracted to repair/replace equipment within nominated timeframes.	NFM/Operator
9	Poor screening of contractors, vendors and people into wholesale and retail areas	Development of security procedures. Physical and electronic security measures to provide access control into restricted areas. . Authorised persons to be provided with appropriate identification (ie ID passes etc).	NFM/Operator
10	Intrusion of non-accredited people into secure areas within the Precinct.	Physical and electronic security measures to provide access control into restricted areas. Security to be provided at key points to visually confirm whether a person is authorised to enter secure area. Authorised persons to be provided with appropriate identification (ie ID passes etc).	NFM/Operator
11	Protest (Staff, Vendors) - Non-Violent	Appropriate policies and procedures are necessary to enable staff to deal with such incidents in an efficient and timely manner, so as to keep the event uninterrupted. These procedures would include liaison with Police and the protest groups (in the event of a planned and announced protest). Protests and demonstrations are to be kept under supervision by both CCTV and security guards.	NFM/Operator
12	Inappropriate management and storage of security related information	Security related information to be stored according to NFM/Facility Information Security Management Plan, Policies and Procedures. Security related information to be securely stored. Security related information to be disseminated on a 'need to know' basis only. Offices to be provided with electronic access control to control and audit access into these areas. Offices to be monitored by PIR's to detect unauthorised access.	NFM/Operator
13	Unauthorised obtainment of access card	Lost/stolen access cards to be reported immediately to the Security Manager/System administrator. Lost/stolen cards to be deprogrammed from the system. Each person issued with an access card is to sign terms and conditions notifying them of their responsibilities regarding the access card. The requirement to immediately report lost/stolen access cards to be included as a term and condition of provision of access card.	NFM/Operator

#	Key Identified Risks	Treatment	Action By
14	Failure to manage and monitor vehicles into and around the Centre	Vehicle management strategy to be in place to control access of vehicles in and around facilities and Precinct. Staff to receive security awareness training in order to increase the likelihood of identification and notification of suspicious activity. CCTV to provide general coverage of Precinct.	NFM/Operator
15	Introduction of Contraband	Screening of persons to be implemented on an as needs basis or randomly. Bag and/or container searches may be required at the where the likelihood of contraband (eg drugs, weapons etc) being brought into the facility is higher.	NFM/Operator
16	Compromise of key system	Keys to be kept in a electronic key cabinet and managed by a key management system which is fully restricted to authorised users and provide audit trails.	NFM/Operator
17	Insider assistance	Staff and contractors to be adequately interviewed and screened prior to employment. The level of screening and background checks will be dependant on the areas that they will be working at. Security/police checks may be required for some high risk areas i.e. security control room, maintenance, cash handling etc.	NFM/Operator
18	Failure to provide necessary escape paths during emergencies	Emergency evacuation routes and provisions to be designed to BCA requirements. Additional requirements may be required on an event by event basis or during peak trading days, and these are to be developed in that security management plan.	NFM/Operator
19	Receipt of Suspect Substances - Containers (biological agents, contraband etc)	Ensure all emergency and incident management procedures are in-place and regularly tested. Continually review and assess risk in coordination with HAZMAT and emergency service departments	NFM/Operator
20	Murder / Manslaughter	Responsible service of alcohol within Precinct restaurants. Removal of inebriated/violent/aggressive patrons from Precinct. Provision of CCTV coverage and security lighting to provide deterrence, surveillance and evidence capturing. On site security presence to respond/diffuse situations. Physical and electronic security measures to control the access of persons into and throughout the Precinct and individual facilities, and to restrict unauthorised access. Incorporation of CPTED strategies of natural access control, natural surveillance and territorial reinforcement to reduce the incidence of crime occurring within the Precinct/Facilities. Help Point to be provided within Public Realm and car park to allow persons to contact the Security Control Room in emergency situations. On-site security to provide response.	NFM/Operator
21	Physical assault	Responsible service of alcohol within Precinct. Removal of inebriated/violent/aggressive patrons from Precinct. Provision of CCTV coverage and security lighting to provide deterrence, surveillance and evidence capturing. On site security presence to respond/diffuse situations. Physical and electronic security measures to control the access of persons into and throughout the Precinct and individual facilities, and to restrict unauthorised access. Incorporation of CPTED strategies of natural access control, natural surveillance and territorial reinforcement to reduce the incidence of crime occurring within the Precinct/Facilities. Help Point to be provided within Public Realm and car park to allow persons to contact the Security Control Room in emergency situations. On-site security to provide response. Fixed duress alarms to be provided in key public contact points and high risk areas.	NFM/Operator
22	Verbal assault	Responsible service of alcohol within Precinct. Removal of inebriated/violent/aggressive patrons from Precinct. Provision of CCTV coverage and security lighting to provide deterrence, surveillance and evidence capturing. On site security presence to respond/diffuse situations. Physical and electronic security measures to control the access of persons into and throughout the Precinct and individual facilities, and to restrict unauthorised access. Incorporation of CPTED strategies of natural access control, natural surveillance and territorial reinforcement to reduce the incidence of crime occurring within the Precinct/Facilities. Help Point to be provided within Public Realm and car park to allow persons to contact the Security Control Room in emergency situations. On-site security to provide response. Fixed duress alarms to be provided in key public contact points and high risk areas.	NFM/Operator

#	Key Identified Risks	Treatment	Action By
23	Sexual assault	Responsible service of alcohol within Precinct. Removal of inebriated/violent/aggressive patrons from Precinct. Provision of CCTV coverage and security lighting to provide deterrence, surveillance and evidence capturing. On site security presence to respond/diffuse situations. Physical and electronic security measures to control the access of persons into and throughout the Precinct and individual facilities, and to restrict unauthorised access. Incorporation of CPTED strategies of natural access control, natural surveillance and territorial reinforcement to reduce the incidence of crime occurring within the Precinct/Facilities. Help Point to be provided within Public Realm and car park to allow persons to contact the Security Control Room in emergency situations. On-site security to provide response. Fixed duress alarms to be provided in key public contact points and high risk areas such as ticket/box office, reception, registration counters, treasury etc.	NFM/Operator
24	Indecent assault	Responsible service of alcohol within Precinct. Removal of inebriated/violent/aggressive patrons from Precinct. Provision of CCTV coverage and security lighting to provide deterrence, surveillance and evidence capturing. On site security presence to respond/diffuse situations. Physical and electronic security measures to control the access of persons into and throughout the Precinct and individual facilities, and to restrict unauthorised access. Incorporation of CPTED strategies of natural access control, natural surveillance and territorial reinforcement to reduce the incidence of crime occurring within the Precinct/Facilities. Help Point to be provided within Public Realm and car park to allow persons to contact the Security Control Room in emergency situations. On-site security to provide response. Fixed duress alarms to be provided in key public contact points and high risk areas.	NFM/Operator
25	Offensive conduct	Responsible service of alcohol within Precinct. Removal of inebriated/violent/aggressive patrons from Precinct. Provision of CCTV coverage and security lighting to provide deterrence, surveillance and evidence capturing. On site security presence to respond/diffuse situations. Physical and electronic security measures to control the access of persons into and throughout the Precinct and individual facilities, and to restrict unauthorised access. Incorporation of CPTED strategies of natural access control, natural surveillance and territorial reinforcement to reduce the incidence of crime occurring within the Precinct/Facilities. Help Point to be provided within Public Realm and car park to allow persons to contact the Security Control Room in emergency situations. On-site security to provide response. Fixed duress alarms to be provided in key public contact points and high risk areas.	NFM/Operator
26	Abduction and kidnapping	Electronic, physical and procedural security measures to restrict/control access into and throughout Precinct/Facilities. Traffic management plan and traffic barriers to restrict/control vehicular access into and throughout Precinct and Facilities. Provide CCTV, natural surveillance and security lighting to provide deterrence, increase the likelihood of detection and provide evidence capturing capabilities. Develop security management procedures outlining the reporting and recording of incident. Police to be notified immediately of situation. Help Points to be provided within Public Realm and Car Park to allow persons to contact the Security Control Room in emergency situations.	NFM/Operator
27	Harassment, threatening behaviour and private nuisance. Staff/Contractors/General Public	Separation of wholesale areas from general public through physical, electronic and procedural security measures. NFM areas to be well lit to aid natural and electronic surveillance and to provide deterrence.	NFM/Operator
28	Robbery - Staff/contractors/public	Security lighting and CCTV surveillance to provide deterrence and to provide a quality recording of the incident which can be used for post event analysis and prosecution purposes. Implement CPTED measures such as providing clear sight lines and low level barriers to provide natural surveillance. Emergency Help Point to be provided within Public Realm. Produce reporting and response procedures for NFM staff. On site security presence to provide response. Physical, electronic and procedural security measures to control access into and throughout Precinct and Facilities. Duress alarms to be installed at high risk areas.	NFM/Operator

#	Key Identified Risks	Treatment	Action By
29	General Theft - organised crime	Security lighting and CCTV surveillance to provide deterrence and to provide a quality recording of the incident which can be used for post event analysis and prosecution purposes. Implement CPTED measures such as providing clear sight lines and low level barriers to provide natural surveillance. Emergency Help Point to be provided within Public Realm. Produce reporting and response procedures for NFM staff. On site security presence to provide response. Physical, electronic and procedural security measures to control access into and throughout Precinct and Facilities.	NFM/Operator
30	General Theft - individual / opportunist	Security lighting and CCTV surveillance to provide deterrence and to provide a quality recording of the incident which can be used for post event analysis and prosecution purposes. Implement CPTED measures such as providing clear sight lines and low level barriers to provide natural surveillance. Emergency Help Point to be provided within Public Realm. Produce reporting and response procedures for NFM staff. On site security presence to provide response. Physical, electronic and procedural security measures to control access into and throughout Precinct and Facilities. Restrict unthorised access to high secure areas.	NFM/Operator
31	Theft of equipment/assets from AV equipment display screens /POS terminals	Provision of electronic access control to restrict unauthorised access, and to provide an audit of authorised access which provides a deterrence. Asset management for the AV equipmment, POS terminals, scales etc.	NFM/Operator
32	Theft from dangerous goods/chemical stores	Provision of electronic access control to restrict unauthorised access, and to provide an audit of authorised access which provides a deterrence. Provision of magnetic reed switches to monitor the integrity of the doors to these locations and signage to deter intruders.	NFM/Operator
33	Theft from Secure Storage	Provision of electronic access control to restrict unauthorised access, and to provide an audit of authorised access which provides a deterrence. Provision of magnetic reed switches to monitor the integrity of the doors to these locations.	NFM/Operator
34	Liquor offences	Sjy bar & restaurent staff/security to check patrons ID before the sale of alcohol. CCTV coverage of restaurent seating areas to provide general surveillance of crowd behaviour. Excessively inebriated patrons to be evicted from premises in accordance with liquor licensing requirements. All staff to be trained/briefed on the Facilities duty of care requirements in relation to the service of alcohol & management of inebriated patrons.	NFM/Operator
35	Hand placed IED, Personal Borne - Improvised Explosive Devices (PBIED's), Vehicle Borne - Improvised Explosive Devices (VBIED's) and Chemical/Biological threats	Development and implementation of business continuity management policies and procedures. Development of emergency evacuation and response policies and procedures. Liaise and coordinate emergency services response and strategy. Develop procedures to handle identified unattended/suspicious items.	NFM/Operator/ Federal & State Government/Emergency Services
		Liaise with State/Federal Security & Intelligence Agencies on regular basis to obtain credible intelligence and Threat assessment updates on likely threat types.	NFM/Operator/ Federal & State Government/Emergency Services
		Train all staff to be aware of threat and report suspicious incidents promptly. Maintaining clear open spaces to minimise concealment and ensure left items are isolated and dealt with promptly. Maintaining an overt security presence will increase the likelihood of halting possible threats. Security and permanent staff to be trained in emergency response procedures in order to improve evacuation and response to specific threat scenarios. Highly overt presence during busy trading periods.	NFM/Operator/ Federal & State Government/Emergency Services
36	Active shooter	Liaise with State/Federal Security & Intelligence Agencies on regular basis to obtain credible intelligence and Threat assessment updates on likely threat types.	NFM/Operator/ Federal & State Government/Emergency Services
		Development and implementation of security policies and procedures. Development of emergency evacuation and response policies and procedures. Liaise and coordinate emergency services response and strategy.	NFM/Operator/ Federal & State Government/Emergency Services



#	Key Identified Risks	Treatment	Action By
		Electronic, physical and procedural security measures to restrict/control access into and throughout Precinct/Facilities. CCTV and security lighting to provide surveillance of Precinct.	NFM/Operator/ Federal & State Government/Emergency Services
37	Bomb threat (hoax and real)	Development and implementation of security policies and procedures. Development of emergency evacuation and response policies and procedures. Liaise and coordinate emergency services response and strategy.	NFM/Operator/ Federal & State Government/Emergency Services
38	Vandalism / graffiti - Criminals/gangs/youths/opportunists	Security lighting, CCTV surveillance and security signage to provide deterrence to criminal behaviour. On site Security guards to respond to incidences and to provide a deterrence. Implement CPTED strategies including clear sight lines, good natural surveillance, natural access control and territorial reinforcement. Timely repair of damage/graffiti.	NFM/Operator
39	Arson	Design all fire and emergency services to code (eg FIP, EWIS, Fire Control Room, Fire suppressions systems, etc). Develop emergency evacuation policies and procedures. Train nominated staff as fire wardens.	NFM/Operator/ Federal & State Government/Emergency Services
		Physical and electronic access control measures to be provided to restrict unauthorised access to Precinct/Facilities. Intruder detection system (PIR's/Reed Switches) to be provided to monitor the integrity of nominated locations, and to notify the Security Control Room of unauthorised access to these locations.	NFM/Operator
40	Espionage - Industrial	Physical and electronic access control measures to be provided to restrict unauthorised access to Precinct/Facilities. Intruder detection system (PIR's/Reed Switches) to be provided to monitor the integrity of nominated locations, and to notify the Security Control Room of unauthorised access to these locations. 'Need to go' principle to be implemented to	NFM/Operator
41	Sabotage	Physical and electronic access control measures to be provided to restrict unauthorised access to Precinct/Facilities. Intruder detection system (PIR's/Reed Switches) to be provided to monitor the integrity of nominated locations, and to notify the Security Control Room of unauthorised access to these locations. Provide required levels of redundancies to critical infrastructure and back ups of critical information.	NFM/Operator
42	Loss of Power or Building Services	Critical services to be supplied with UPS/backup generators. Plant rooms to be key locked and have reed switches fitted to prevent unauthorised and undetected access to plant and equipment.	NFM/Operator/Contractors
43	Physical attack against IT or Communications infrastructure	Implement an adequate level of system redundancies and system backups. Physical, electronic and procedural security measures to control and restrict access to critical infrastructure. Robust IT security measures implemented to protect against online attack of infrastructure.	NFM/Operator/Cyber Security personnel
		Provide access control/reed switches/ mechanical locking to communications rooms/risers to control access. Monitor these locations for unauthorised or forced entry.	NFM/Operator/Contractors
44	Information / data resources	Adequate IT security measures to be provided to protect IT infrastructure and NFM information against attack. Perform regular back ups of data.	NFM/Operator/Contractors
45	Unauthorised or inadvertent disclosure of sensitive information	Sensitive information to be stored according to NFM/Facility Information Security Management Plan, Policies and Procedures. Sensitive information to be securely stored. Sensitive information to be disseminated on a 'need to know' basis only. Offices to be provided with electronic access control to control and audit access into these areas. Offices to be monitored by PIR's to detect unauthorised access.	NFM/Operator



#	Key Identified Risks	Treatment	Action By
46	Unauthorised Access to Security Head-End Equipment	Communications rooms to be provided with electronic access control. Security head-end to be installed within dedicated communications racks. Main security head-end equipment to be installed within a dedicated security comms room within the Security Control Room.	NFM/Operator
47	Theft from building, property, assets, theft from vehicle and theft of vehicle	Provision of CCTV coverage and natural surveillance. Restrict unauthorised access. Provide suitable signage within the car parks.	NFM/Operator
48	Theft from dangerous goods/chemical stores	Provision of electronic access control to restrict unauthorised access, and to provide an audit of authorised access which provides a deterrent. Provision of magnetic reed switches to monitor the integrity of the doors to these locations. Provide suitable signage.	NFM/Operator
49	Break and Enter, Burglary	Provision of electronic access control, natural and electronic surveillance to restrict and monitor unauthorised access. Provision of magnetic reed switches and PIRs to monitor intruder detection.	NFM/Operator

# Appendix B

## Security Treatment Matrix

## Security Risk - Treatment Register

#	Key Identified Risks	Treatment	Action By
1	Facility Location & Exposure	Due to the location, profile and media exposure of NFM, a flexible and scalable security solution will need to be provided in order to adequately treat the diverse range of risks the Precinct is likely to be exposed to. The following Precinct wide treatment measures should be provided;	NFM/Operator
		Installation of appropriate Precinct lighting to ensure CCTV has clear view of any activity within the Public Realm, and to assist natural surveillance.	NFM/Operator
		Installation of Precinct CCTV Cameras to provide general surveillance of the Precinct, and to provide deterrence to antisocial/criminal behaviour. An emergency help point system should be considered within the Public Realm to allow members of the public to contact the Security Control Room in emergency situations. Mobile security guards should be provided to perform a roaming patrol of the Precinct and to provide a response to security situations. The number of mobile security guards to be determined based on the risk profile of the current events being held within the Precinct at that point in time.	NFM/Operator
		Crime prevention through environmental design (CPTED) principals should be incorporated into the Precinct layout and landscaping. The Precinct design should enhance natural surveillance by providing clear sight lines and eliminating areas of concealment, provide natural access control and promote territorial reinforcement.	NFM/Operator
2	Unauthorised Access - Pedestrian	Implementation of appropriate staff identification cards and electronic access control to the Facilities/Precent, and to sensitive or key areas within each Facility. Physical security measures to control access into and throughout the Precinct and Facilities. Creation of check points during events to restrict unauthorised access into Precinct/Facilities/areas within facilities. Provision of intrusion detection system to monitor key areas of facilities and to detect unauthorised access to these areas. On site security to provide a timely and appropriate response to unauthorised access.	NFM/Operator
3	Unauthorised Access - Vehicle	For high risk, high profile events where high profile dignitaries etc will be present NFM security will be required to liaise with and coordinate security requirements with relevant security organisations (eg NSW Police, AFP representatives).	NFM/Operator
		During high risk events, additional vehicle access control mechanisms, such as vehicle check points should be created where credentials and other bona fides are assessed prior to gaining entry to the site/next check point. Higher risk events should implement a 'Defence in Depth' approach to perimeter security consisting of concentric layers of security barriers with check points at each barrier.	NFM/Operator
		As part of the permanent security provisions for NFM, an appropriate security gate/entry barrier/boom gates should be provided in nominated locations to deter and delay unauthorised vehicles from accessing the site. These devices should be used in conjunction with other vehicular control devices such as perimeter fences, curbing, bollards and natural access control (CPTED) strategies. Intercoms with remote door release functionality and electronic access control should also be provided at the security gate/entry barrier to allow authorised access.	NFM/Operator
		Ensure that the only vehicles required on site are those of making deliveries and NFM vehicles, which will enable a clearer and swifter identification of unauthorised vehicles. This vehicular control strategy will involve staff and the general public only being able to access the public car park.	NFM/Operator
		As the NFM Precent is largely an open design, boom gates/gates will predominantly be installed at car park entry/exit points, and the entry/exit points to loading docks and the secure service yard.	NFM/Operator

#	Key Identified Risks	Treatment	Action By
4	Forced Access - Pedestrian	Physical and electronic access control measures to be provided to restrict unauthorised access to Precinct/Facilities. Intruder detection system (PIR's/Reed Switches) to be provided to monitor the integrity of nominated locations, and to notify the Security Control Room of a breach.	NFM/Operator
5	Forced Access - Vehicle	Portable anti-ram vehicle barriers may be required for specific high risk events based on the events' risk profile.	NFM/Operator
6	Unauthorised Access - Waterborne	Sydney Harbour Foreshore Authority and the Water Police will need to be liaised and coordinated with in order to provide monitoring and restricted zones in the Harbour. The Harbour itself provides a level of natural access control. Lighting and CCTV will be required along the Harbour side of the Precinct to improve surveillance of this area and deter intruders. Integrated signage to depict restricted access to the Wharf terminals should be considered.	NFM/Operator
7	Mechanical failure of security equipment	Implement a regular maintenance regime, redundancies and system back ups/spare equipment to be provided in accordance with Australian standards and industry best practice. Contractors responsible for repair/replacement of failed equipment to be contracted to repair/replace equipment within nominated timeframes.	NFM/Operator
8	Mechanical failure critical building services/equipment	Implement a regular maintenance regime, redundancies and system back ups/spare equipment to be provided in accordance with Australian standards and industry best practice. Contractors responsible for repair/replacement of failed equipment to be contracted to repair/replace equipment within nominated timeframes.	NFM/Operator
9	Poor screening of contractors, vendors and people into wholesale and retail areas	Development of security procedures. Physical and electronic security measures to provide access control into restricted areas. . Authorised persons to be provided with appropriate identification (ie ID passes etc).	NFM/Operator
10	Intrusion of non-accredited people into secure areas within the Precinct.	Physical and electronic security measures to provide access control into restricted areas. Security to be provided at key points to visually confirm whether a person is authorised to enter secure area. Authorised persons to be provided with appropriate identification (ie ID passes etc).	NFM/Operator
11	Protest (Staff, Vendors) - Non-Violent	Appropriate policies and procedures are necessary to enable staff to deal with such incidents in an efficient and timely manner, so as to keep the event uninterrupted. These procedures would include liaison with Police and the protest groups (in the event of a planned and announced protest). Protests and demonstrations are to be kept under supervision by both CCTV and security guards.	NFM/Operator
12	Inappropriate management and storage of security related information	Security related information to be stored according to NFM/Facility Information Security Management Plan, Policies and Procedures. Security related information to be securely stored. Security related information to be disseminated on a 'need to know' basis only. Offices to be provided with electronic access control to control and audit access into these areas. Offices to be monitored by PIR's to detect unauthorised access.	NFM/Operator
13	Unauthorised obtainment of access card	Lost/stolen access cards to be reported immediately to the Security Manager/System administrator. Lost/stolen cards to be deprogrammed from the system. Each person issued with an access card is to sign terms and conditions notifying them of their responsibilities regarding the access card. The requirement to immediately report lost/stolen access cards to be included as a term and condition of provision of access card.	NFM/Operator

#	Key Identified Risks	Treatment	Action By
14	Failure to manage and monitor vehicles into and around the Centre	Vehicle management strategy to be in place to control access of vehicles in and around facilities and Precinct. Staff to receive security awareness training in order to increase the likelihood of identification and notification of suspicious activity. CCTV to provide general coverage of Precinct.	NFM/Operator
15	Introduction of Contraband	Screening of persons to be implemented on an as needs basis or randomly. Bag and/or container searches may be required at the where the likelihood of contraband (eg drugs, weapons etc) being brought into the facility is higher.	NFM/Operator
16	Compromise of key system	Keys to be kept in a electronic key cabinet and managed by a key management system which is fully restricted to authorised users and provide audit trails.	NFM/Operator
17	Insider assistance	Staff and contractors to be adequately interviewed and screened prior to employment. The level of screening and background checks will be dependant on the areas that they will be working at. Security/police checks may be required for some high risk areas i.e. security control room, maintenance, cash handling etc.	NFM/Operator
18	Failure to provide necessary escape paths during emergencies	Emergency evacuation routes and provisions to be designed to BCA requirements. Additional requirements may be required on an event by event basis or during peak trading days, and these are to be developed in that security management plan.	NFM/Operator
19	Receipt of Suspect Substances - Containers (biological agents, contraband etc)	Ensure all emergency and incident management procedures are in-place and regularly tested. Continually review and assess risk in coordination with HAZMAT and emergency service departments	NFM/Operator
20	Murder / Manslaughter	Responsible service of alcohol within Precinct restaurants. Removal of inebriated/violent/aggressive patrons from Precinct. Provision of CCTV coverage and security lighting to provide deterrence, surveillance and evidence capturing. On site security presence to respond/diffuse situations. Physical and electronic security measures to control the access of persons into and throughout the Precinct and individual facilities, and to restrict unauthorised access. Incorporation of CPTED strategies of natural access control, natural surveillance and territorial reinforcement to reduce the incidence of crime occurring within the Precinct/Facilities. Help Point to be provided within Public Realm and car park to allow persons to contact the Security Control Room in emergency situations. On-site security to provide response.	NFM/Operator
21	Physical assault	Responsible service of alcohol within Precinct. Removal of inebriated/violent/aggressive patrons from Precinct. Provision of CCTV coverage and security lighting to provide deterrence, surveillance and evidence capturing. On site security presence to respond/diffuse situations. Physical and electronic security measures to control the access of persons into and throughout the Precinct and individual facilities, and to restrict unauthorised access. Incorporation of CPTED strategies of natural access control, natural surveillance and territorial reinforcement to reduce the incidence of crime occurring within the Precinct/Facilities. Help Point to be provided within Public Realm and car park to allow persons to contact the Security Control Room in emergency situations. On-site security to provide response. Fixed duress alarms to be provided in key public contact points and high risk areas.	NFM/Operator
22	Verbal assault	Responsible service of alcohol within Precinct. Removal of inebriated/violent/aggressive patrons from Precinct. Provision of CCTV coverage and security lighting to provide deterrence, surveillance and evidence capturing. On site security presence to respond/diffuse situations. Physical and electronic security measures to control the access of persons into and throughout the Precinct and individual facilities, and to restrict unauthorised access. Incorporation of CPTED strategies of natural access control, natural surveillance and territorial reinforcement to reduce the incidence of crime occurring within the Precinct/Facilities. Help Point to be provided within Public Realm and car park to allow persons to contact the Security Control Room in emergency situations. On-site security to provide response. Fixed duress alarms to be provided in key public contact points and high risk areas.	NFM/Operator

#	Key Identified Risks	Treatment	Action By
23	Sexual assault	Responsible service of alcohol within Precinct. Removal of inebriated/violent/aggressive patrons from Precinct. Provision of CCTV coverage and security lighting to provide deterrence, surveillance and evidence capturing. On site security presence to respond/diffuse situations. Physical and electronic security measures to control the access of persons into and throughout the Precinct and individual facilities, and to restrict unauthorised access. Incorporation of CPTED strategies of natural access control, natural surveillance and territorial reinforcement to reduce the incidence of crime occurring within the Precinct/Facilities. Help Point to be provided within Public Realm and car park to allow persons to contact the Security Control Room in emergency situations. On-site security to provide response. Fixed duress alarms to be provided in key public contact points and high risk areas such as ticket/box office, reception, registration counters, treasury etc.	NFM/Operator
24	Indecent assault	Responsible service of alcohol within Precinct. Removal of inebriated/violent/aggressive patrons from Precinct. Provision of CCTV coverage and security lighting to provide deterrence, surveillance and evidence capturing. On site security presence to respond/diffuse situations. Physical and electronic security measures to control the access of persons into and throughout the Precinct and individual facilities, and to restrict unauthorised access. Incorporation of CPTED strategies of natural access control, natural surveillance and territorial reinforcement to reduce the incidence of crime occurring within the Precinct/Facilities. Help Point to be provided within Public Realm and car park to allow persons to contact the Security Control Room in emergency situations. On-site security to provide response. Fixed duress alarms to be provided in key public contact points and high risk areas.	NFM/Operator
25	Offensive conduct	Responsible service of alcohol within Precinct. Removal of inebriated/violent/aggressive patrons from Precinct. Provision of CCTV coverage and security lighting to provide deterrence, surveillance and evidence capturing. On site security presence to respond/diffuse situations. Physical and electronic security measures to control the access of persons into and throughout the Precinct and individual facilities, and to restrict unauthorised access. Incorporation of CPTED strategies of natural access control, natural surveillance and territorial reinforcement to reduce the incidence of crime occurring within the Precinct/Facilities. Help Point to be provided within Public Realm and car park to allow persons to contact the Security Control Room in emergency situations. On-site security to provide response. Fixed duress alarms to be provided in key public contact points and high risk areas.	NFM/Operator
26	Abduction and kidnapping	Electronic, physical and procedural security measures to restrict/control access into and throughout Precinct/Facilities. Traffic management plan and traffic barriers to restrict/control vehicular access into and throughout Precinct and Facilities. Provide CCTV, natural surveillance and security lighting to provide deterrence, increase the likelihood of detection and provide evidence capturing capabilities. Develop security management procedures outlining the reporting and recording of incident. Police to be notified immediately of situation. Help Points to be provided within Public Realm and Car Park to allow persons to contact the Security Control Room in emergency situations.	NFM/Operator
27	Harassment, threatening behaviour and private nuisance. Staff/Contractors/General Public	Separation of wholesale areas from general public through physical, electronic and procedural security measures. NFM areas to be well lit to aid natural and electronic surveillance and to provide deterrence.	NFM/Operator
28	Robbery - Staff/contractors/public	Security lighting and CCTV surveillance to provide deterrence and to provide a quality recording of the incident which can be used for post event analysis and prosecution purposes. Implement CPTED measures such as providing clear sight lines and low level barriers to provide natural surveillance. Emergency Help Point to be provided within Public Realm. Produce reporting and response procedures for NFM staff. On site security presence to provide response. Physical, electronic and procedural security measures to control access into and throughout Precinct and Facilities. Duress alarms to be installed at high risk areas.	NFM/Operator

#	Key Identified Risks	Treatment	Action By
29	General Theft - organised crime	Security lighting and CCTV surveillance to provide deterrence and to provide a quality recording of the incident which can be used for post event analysis and prosecution purposes. Implement CPTED measures such as providing clear sight lines and low level barriers to provide natural surveillance. Emergency Help Point to be provided within Public Realm. Produce reporting and response procedures for NFM staff. On site security presence to provide response. Physical, electronic and procedural security measures to control access into and throughout Precinct and Facilities.	NFM/Operator
30	General Theft - individual / opportunist	Security lighting and CCTV surveillance to provide deterrence and to provide a quality recording of the incident which can be used for post event analysis and prosecution purposes. Implement CPTED measures such as providing clear sight lines and low level barriers to provide natural surveillance. Emergency Help Point to be provided within Public Realm. Produce reporting and response procedures for NFM staff. On site security presence to provide response. Physical, electronic and procedural security measures to control access into and throughout Precinct and Facilities. Restrict unthorised access to high secure areas.	NFM/Operator
31	Theft of equipment/assets from AV equipment display screens /POS terminals	Provision of electronic access control to restrict unauthorised access, and to provide an audit of authorised access which provides a deterrence. Asset management for the AV equipmment, POS terminals, scales etc.	NFM/Operator
32	Theft from dangerous goods/chemical stores	Provision of electronic access control to restrict unauthorised access, and to provide an audit of authorised access which provides a deterrence. Provision of magnetic reed switches to monitor the integrity of the doors to these locations and signage to deter intruders.	NFM/Operator
33	Theft from Secure Storage	Provision of electronic access control to restrict unauthorised access, and to provide an audit of authorised access which provides a deterrence. Provision of magnetic reed switches to monitor the integrity of the doors to these locations.	NFM/Operator
34	Liquor offences	Sjy bar & restaurent staff/security to check patrons ID before the sale of alcohol. CCTV coverage of restaurent seating areas to provide general surveillance of crowd behaviour. Excessively inebriated patrons to be evicted from premises in accordance with liquor licensing requirements. All staff to be trained/briefed on the Facilities duty of care requirements in relation to the service of alcohol & management of inebriated patrons.	NFM/Operator
35	Hand placed IED, Personal Borne - Improvised Explosive Devices (PBIED's), Vehicle Borne - Improvised Explosive Devices (VBIED's) and Chemical/Biological threats	Development and implementation of business continuity management policies and procedures. Development of emergency evacuation and response policies and procedures. Liaise and coordinate emergency services response and strategy. Develop procedures to handle identified unattended/suspicious items.	NFM/Operator/ Federal & State Government/Emergency Services
		Liaise with State/Federal Security & Intelligence Agencies on regular basis to obtain credible intelligence and Threat assessment updates on likely threat types.	NFM/Operator/ Federal & State Government/Emergency Services
		Train all staff to be aware of threat and report suspicious incidents promptly. Maintaining clear open spaces to minimise concealment and ensure left items are isolated and dealt with promptly. Maintaining an overt security presence will increase the likelihood of halting possible threats. Security and permanent staff to be trained in emergency response procedures in order to improve evacuation and response to specific threat scenarios. Highly overt presence during busy trading periods.	NFM/Operator/ Federal & State Government/Emergency Services
36	Active shooter	Liaise with State/Federal Security & Intelligence Agencies on regular basis to obtain credible intelligence and Threat assessment updates on likely threat types.	NFM/Operator/ Federal & State Government/Emergency Services
		Development and implementation of security policies and procedures. Development of emergency evacuation and response policies and procedures. Liaise and coordinate emergency services response and strategy.	NFM/Operator/ Federal & State Government/Emergency Services



#	Key Identified Risks	Treatment	Action By
		Electronic, physical and procedural security measures to restrict/control access into and throughout Precinct/Facilities. CCTV and security lighting to provide surveillance of Precinct.	NFM/Operator/ Federal & State Government/Emergency Services
37	Bomb threat (hoax and real)	Development and implementation of security policies and procedures. Development of emergency evacuation and response policies and procedures. Liaise and coordinate emergency services response and strategy.	NFM/Operator/ Federal & State Government/Emergency Services
38	Vandalism / graffiti - Criminals/gangs/youths/opportunists	Security lighting, CCTV surveillance and security signage to provide deterrence to criminal behaviour. On site Security guards to respond to incidences and to provide a deterrence. Implement CPTED strategies including clear sight lines, good natural surveillance, natural access control and territorial reinforcement. Timely repair of damage/graffiti.	NFM/Operator
39	Arson	Design all fire and emergency services to code (eg FIP, EWIS, Fire Control Room, Fire suppressions systems, etc). Develop emergency evacuation policies and procedures. Train nominated staff as fire wardens.	NFM/Operator/ Federal & State Government/Emergency Services
		Physical and electronic access control measures to be provided to restrict unauthorised access to Precinct/Facilities. Intruder detection system (PIR's/Reed Switches) to be provided to monitor the integrity of nominated locations, and to notify the Security Control Room of unauthorised access to these locations.	NFM/Operator
40	Espionage - Industrial	Physical and electronic access control measures to be provided to restrict unauthorised access to Precinct/Facilities. Intruder detection system (PIR's/Reed Switches) to be provided to monitor the integrity of nominated locations, and to notify the Security Control Room of unauthorised access to these locations. 'Need to go' principle to be implemented to	NFM/Operator
41	Sabotage	Physical and electronic access control measures to be provided to restrict unauthorised access to Precinct/Facilities. Intruder detection system (PIR's/Reed Switches) to be provided to monitor the integrity of nominated locations, and to notify the Security Control Room of unauthorised access to these locations. Provide required levels of redundancies to critical infrastructure and back ups of critical information.	NFM/Operator
42	Loss of Power or Building Services	Critical services to be supplied with UPS/backup generators. Plant rooms to be key locked and have reed switches fitted to prevent unauthorised and undetected access to plant and equipment.	NFM/Operator/Contractors
43	Physical attack against IT or Communications infrastructure	Implement an adequate level of system redundancies and system backups. Physical, electronic and procedural security measures to control and restrict access to critical infrastructure. Robust IT security measures implemented to protect against online attack of infrastructure.	NFM/Operator/Cyber Security personnel
		Provide access control/reed switches/ mechanical locking to communications rooms/risers to control access. Monitor these locations for unauthorised or forced entry.	NFM/Operator/Contractors
44	Information / data resources	Adequate IT security measures to be provided to protect IT infrastructure and NFM information against attack. Perform regular back ups of data.	NFM/Operator/Contractors
45	Unauthorised or inadvertent disclosure of sensitive information	Sensitive information to be stored according to NFM/Facility Information Security Management Plan, Policies and Procedures. Sensitive information to be securely stored. Sensitive information to be disseminated on a 'need to know' basis only. Offices to be provided with electronic access control to control and audit access into these areas. Offices to be monitored by PIR's to detect unauthorised access.	NFM/Operator



#	Key Identified Risks	Treatment	Action By
46	Unauthorised Access to Security Head-End Equipment	Communications rooms to be provided with electronic access control. Security head-end to be installed within dedicated communications racks. Main security head-end equipment to be installed within a dedicated security comms room within the Security Control Room.	NFM/Operator
47	Theft from building, property, assets, theft from vehicle and theft of vehicle	Provision of CCTV coverage and natural surveillance. Restrict unauthorised access. Provide suitable signage within the car parks.	NFM/Operator
48	Theft from dangerous goods/chemical stores	Provision of electronic access control to restrict unauthorised access, and to provide an audit of authorised access which provides a deterrence. Provision of magnetic reed switches to monitor the integrity of the doors to these locations. Provide suitable signage.	NFM/Operator
49	Break and Enter, Burglary	Provision of electronic access control, natural and electronic surveillance to restrict and monitor unauthorised access. Provision of magnetic reed switches and PIRs to monitor intruder detection.	NFM/Operator