

# Security Risk Assessment Report

NeW Space



**D R A F T**

## Security Risk Assessment Report

NeW Space

Client: University of Newcastle

ABN: 15 736 576 735

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

17-Apr-2014

Job No.: 60315005

AECOM in Australia and New Zealand is certified to the latest version of 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.

**DRAFT****Quality Information**

Document      Security Risk Assessment Report

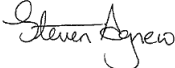
Ref             60315005

Date            17-Apr-2014

Prepared by   Chris Nunn

Reviewed by   Dan Rasins

## Revision History

Revision	Revision Date	Details	Authorised	
			Name/Position	Signature
A	17-Apr-2014	For Information	Steve Agnew Technical Director	

**DRAFT****Table of Contents**

Executive Summary		1
1.0	Introduction	3
	1.1 Purpose	3
	1.2 The Project	3
	1.3 The Site	3
	1.4 Methodology	3
	1.5 Caveat	4
2.0	Security Standards	5
	2.1 General	5
	2.2 International & Australian Standards and Guidelines	5
	2.3 University of Newcastle Standards and Guidelines	6
3.0	Crime Prevention through Environmental Design (CPTED)	7
	3.1 CPTED Theory	7
	3.1.1 General	7
	3.1.2 Natural Access Control	7
	3.1.3 Natural Surveillance	7
	3.1.4 Territorial Reinforcement	7
4.0	Criminological Perspective of Crime	8
	4.1 Purpose	8
	4.2 Definition of Crime	8
	4.3 Criminological Theories	8
	4.3.1 General	8
	4.3.2 Neutralisation (Drift) Theory	8
	4.3.3 Theory of Differential Association	8
	4.3.4 Strain Theory	9
5.0	Security Philosophies & Principles	11
	5.1 General	11
	5.2 Defence in Depth	11
	5.2.1 Outer Layer	11
	5.2.2 Middle Layer	11
	5.2.3 Inner Layers	12
	5.3 Deter, Detect, Delay & Respond (D <sup>3</sup> R) Principle	12
	5.3.1 Deter	12
	5.3.2 Detect	12
	5.3.3 Delay	12
	5.3.4 Response	12
	5.4 Target Hardening	12
	5.5 Situational Crime Prevention	13
6.0	Security Risk Management	14
	6.1 Overview	14
	6.2 Principles	15
	6.3 Framework	16
	6.3.1 General	16
	6.4 Mandate and Commitment	16
	6.5 Process	16
7.0	Security Risk Assessment	18
	7.1 Communication & Consultation	18
	7.2 Context Establishment	18
	7.2.1 External Context	18
	7.2.2 Internal Context	21
	7.3 Risk Identification	21
	7.3.1 Definition of Risk	21
	7.3.2 General	22
	7.3.3 Sources of Threat	22
	7.3.4 Most Prevalent Crimes	22

**DRAFT**

	7.3.5	Highest Ranking Crimes	23
	7.3.6	City of Newcastle LGA Crime Hotspot Map	24
	7.3.7	Crime Analysis	24
7.4		Risk Assessment	26
	7.4.1	Process	26
	7.4.2	Risk Assessment Matrices	26
	7.4.3	Security Risks	28
7.5		Threat Assessment	29
	7.5.1	Threat Overview	29
	7.5.2	Intent	29
	7.5.3	Capability	29
	7.5.4	Measuring the Threat	29
7.6		Risk Analysis	30
	7.6.1	Risk Trend: Trespass	30
	7.6.2	Risk Trend: Antisocial Behaviour	31
	7.6.3	Risk Trend: Vandalism	32
	7.6.4	Risk Trend: Theft & Robbery	33
	7.6.5	Risk Trend: Assault	34
	7.6.6	Risk Trend: Drug and Alcohol Related Offences	35
	7.6.7	Risk Trend: Terrorist Type Activities & Active Shooters	35
7.7		Risk Evaluation	37
	7.7.1	General	37
	7.7.2	Tolerance of Risk	37
7.8		Risk Treatment	38
7.9		Monitoring & Review	39
	7.9.1	Monitoring & Review Practices	39
	7.9.2	Triggering Monitoring & Review Processes	40
	7.9.3	Post Event Analysis & Reporting	40
8.0		Recommendations	42
	8.1	CPTED Measures	42
	8.2	Physical Security Measures	42
	8.3	Electronic Security Measures	42
	8.3.1	EACS	42
	8.3.2	IAS	42
	8.3.3	CCTV	42
	8.3.4	Emergency Help Points and Duress	42
	8.4	Information Security Measures	43
	8.5	Operational Security Measures	43
	8.6	Security Management Measures	43
Appendix A		Security Risk Matrix	A

# DRAFT

## Executive Summary

### Overview and Objective

This Security Risk Assessment (SRA) for the University of Newcastle NeW Space project has been based on the international risk management standard ISO 31000:2009 – Risk Management – Principles and Guidelines. The security risk treatment and mitigation methods recommended within this report are based on Australian Security Standards, current security theories and reasonable industry practices.

### Security Environment

The crime statistics for the Local Government Area (LGA) within which the University of Newcastle (UoN) is located (City of Newcastle) has been reviewed and analysed in order to help define the security environment and define the security related risks that the site will likely be exposed to. The crime rates experienced within the City of Newcastle LGA have also been compared against the crime rates of the other LGA's within the Sydney region.

*The City of Newcastle LGA generally has high to medium rates of crime when compared to the other LGA's within the Sydney region.*

The crime statistics for the City of Newcastle LGA have been analysed, with the following reported crimes (relevant to the project) the most prevalent;

- Malicious damage to property (2,651 offences, #32);
- Steal from a motor vehicle (1,746 offences, #9);
- Assault – non-domestic violence related (1,232 offences, #17);
- Theft (1,164 offences, #13);
- Fraud (1,125 offences, #15);
- Harassment, threatening behaviour and private nuisance (787 offences, #49);
- Motor vehicle theft (667 offences, #8);
- Break and enter non-dwelling (573 offences, #42);
- Liquor Offences (378 offences, #44);
- Offensive Conduct (349 offences, #27);
- Sexual or Indecent Assault (313 offences, #46);
- Possession and/or use of cannabis (307 offences, #85);
- Steal from Person (292 offences, #5);
- Trespass (206 offences, #75);
- Prohibited and regulated weapons offences (196 offences, #69);
- Arson (193 offences, #53);
- Robbery (187 offences, #6);
- Offensive Language (164 offences, #43); and
- Possession and/or use of amphetamines (164 offences).

Through the security risk assessment process, the main security risk trends that the UoN NeW Space building will likely be exposed to that requires treatment are;

- Theft;
- Drug/Alcohol related offences;
- Robbery;

## DRAFT

- Malicious damage to property/Graffiti;
- Assault;
- Trespass; and
- Antisocial Behaviour.

### Recommendations

A broad range of security treatment measures have been recommended in Section 8.0 to help mitigate and treat the identified security risks that the UoN NeW Space building is likely to be exposed to. The recommended security treatment measures are based on Australian Security Standards, current security theories and reasonable security and security risk management practices. Recommended security treatment measures include the use of closed circuit television (CCTV), electronic access control, help point and duress alarm systems, security lighting, and crime prevention through environmental design (CPTED) principles.

# DRAFT

## 1.0 Introduction

### 1.1 Purpose

The purpose of this security risk assessment is to comply with the requirement outlined in Section 5.1 of the University of Newcastle Engineering Services Design Standard, which requires that a security risk analysis and safety evaluation be conducted.

The purpose of this evaluation is to identify the security risks associated with the UoN NeW Space building and to provide treatment measures to lower the risk profile to acceptable levels.

### 1.2 The Project

The NeW Space project comprises a new building on a prominent site at the corner of Auckland and Hunter streets in Newcastle, and alterations to University House.

The new facility will have a role as the gateway building to the Civic and Education Precinct, as an icon for the UoN and for the UoN Faculty of Business and Law. The building and its surrounding streetscape will be a critical element in enhancing the character of the precinct, which will be at the heart of a redeveloped Newcastle.

The project has two integrated components:

- A new building on Lot 1 of the vacant site in accordance with the schedule of accommodation detailed within this document; and
- Works to the ground floor of University House integrating it with the new building to ensure interconnectivity, integration and permeability between the two building elements to provide a single resource.

The project will accommodate the offices and teaching accommodation for the Faculty of Business and Law. The facility will contain a Library and Learning Hub to support Business and Law students and Music students from the nearby Newcastle Conservatorium of Music. The new Library and Learning Hub will also provide support to any UoN students who wish to use it and it is particularly directed at those student living in the central city area.

Fully developed, the NeW Space facility will support face to face teaching for over 3,000 undergraduate (UG) students, many hundreds of post-graduates (PG) and over 300 staff. It is the first UoN building with a significant frontage to Hunter Street, and both UoN and the Newcastle City Council (NCC) are keen for the building to be a prominent and an important part of the Civic Precinct, and a harbinger of the new development that is anticipated along Hunter Street following the removal of the heavy rail line.

### 1.3 The Site

The site for the new building is substantially level and is situated to the North of the existing UoN owned building University House and to the West of the Council owned Civic Theatre. A small park, Christie Park, lies to the south of the site and is to the East of University House.

The buildings previously on the site have already been demolished and the site is substantially ready for construction work to commence. The only remaining elements are concrete slabs and in-ground services.

There are archaeological considerations on the site which are currently being investigated by an archaeologist. The archaeological issues include heritage sandstone footings on the NE corner of the site.

The approximate RL's of Hunter Street and University House are as follows:

- Hunter St: RL 2.50
- Gallery section of University House, adjacent boundary: RL 5.37
- Learning Hub section of University House, adjacent King St: RL 3.825

### 1.4 Methodology

The security risk assessment methodology that has been used has based on the International Standard ISO 31000:2009 – Risk Management – Principles and Guidelines and has been optimised for security risk purposes.



## DRAFT

- Review and analyse the Local Government Area crime statistics within which the Building is located, in order to identify the key security related risks that the site is exposed to;
- Review and analyse the Australian Government Census information in order to gain an understanding of the suburb demographics, to help establish the internal and external environment within which the Building is located and operates in;
- Produce a Draft Security Risk Assessment Report and issue for client comment;
- Report to provide recommendations for CPTED strategies, and physical, electronic and procedural security mitigation treatments for the identified security risks;
- Undertake a Security Risk Assessment Workshop with project Stakeholders to identify, analyse and evaluate/rate the security risks (To occur following the issue of this Draft report);
- During this Workshop the final risk ratings will be agreed upon by the Stakeholders;
- Stakeholder comments will be reviewed and incorporated into the Final revision of the SRA Report where required, as will the outcomes from the SRA Workshop; and
- A final Security Risk Assessment Report will then be issued to the Client.

### 1.5 Caveat

This security risk assessment has been based on the information available at the time of writing. As risks can change rapidly it is recommended that UoN regularly review the risk profile at the NeW Space Building site and act accordingly.

# DRAFT

## 2.0 Security Standards

### 2.1 General

The following sections contain a list of the International and Australian standards, guidelines and handbooks that are relevant to the Security Services designs, specifications and reports produced for this project.

### 2.2 International & Australian Standards and Guidelines

- 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;
- 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;
- Building Code of Australia 2014;
- AS 1428.1-2009 Design for Access and Mobility. Part 1: General Requirements for Access – New Building Work;
- AS/NZS 3000, Wiring Rules;
- AS/NZS 3080, Telecommunications installations – Generic cabling for commercial premises;
- AS/NZS 3084, Telecommunications installations – Telecommunications pathways and spaces for commercial buildings;
- AS/NZS 3085, Telecommunications installations – Administration of Communications cabling systems;
- AS/NZS 4252 Electromagnetic Compatibility – Generic Immunity Standard;
- AS/NZS 4252.1 Electromagnetic Compatibility – Generic Immunity Standard Residential, Commercial and Light Industry;
- AS/NZS 4251.1 Electromagnetic Compatibility (EMC) – Generic Emission Standard Residential, Commercial and Light Industry;
- AS/NZS IEC 61935.1 – Testing of balanced communication cabling in accordance with ISO/IEC 11801, Part.1: Installed cabling;
- AS/NZS IEC 61935.2– Testing of balanced communication cabling in accordance with ISO/IEC 11801, Part.2: Patch cords and work area cords;

## DRAFT

- ISO/IEC 14763-3, Information Technology – Implementation and operation of customer premise cabling – Part 3: Testing of optical fibre cabling;
- ISO/IEC 24702, Information Technology – Generic cabling – Industrial premises;
- AS/ACIF S008, Australian Standard – Requirements for Authorised Cabling Products;
- AS/ACIF S009, Australian Standard – Installation requirements for customer cabling (Wiring Rules);
- 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;
- HB 292 A Practitioners Guide to Business Continuity Management;
- HB 293 Executive Guide to Business Continuity Management; and
- US Department of Homeland Security FEMA Risk Management Series.

### 2.3 University of Newcastle Standards and Guidelines

- The University of Newcastle Engineering Services Design Standard; and
- The University of Newcastle Cardax Electronic Security System Standard.

# DRAFT

## 3.0 Crime Prevention through Environmental Design (CPTED)

### 3.1 CPTED Theory

#### 3.1.1 General

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 UoN NeW Space Building should strive to incorporate the three overlaying CPTED strategies – Natural Access Control, Natural Surveillance and Territorial Reinforcement.

#### 3.1.2 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 improved at the UoN NeW Space 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.

#### 3.1.3 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 UoN NeW Space site, the design and layouts should strive to achieve where practical, clear sight lines, eliminate blind spots/ hiding places/ places for concealment, only use low height vegetation, position high risk areas in areas with good natural surveillance, and ensure the areas are well illuminated. In particular, clear sight lines should be achieved at the UoN NeW Space Building entry/exit.

#### 3.1.4 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 appropriate authorities. 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 UoN NeW Space site by ensuring it is well maintained, kept 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.

# DRAFT

## 4.0 Criminological Perspective of Crime

### 4.1 Purpose

Crime based risks and criminal offenders pose the most likely sources of security risks faced by the UoN NeW Space Building. Therefore, in order to effectively understand and manage the security related risks that the Building is exposed to, it is imperative to gain an understanding of crime and the reasons and motives of why people commit crime. By gaining an understanding of crime, why people commit crime, and what motivates people to commit crime, UoN will be more capable of effectively managing its crime based security risks.

### 4.2 Definition of Crime

Crime is that behaviour which deviates from the norm of acceptable behaviour and causes pain to others, which is against the laws of the land and for which the governing authority has sanctions in place.

Crimes are the types of behaviours and acts for which the state provides formally sanctioned punishments.

### 4.3 Criminological Theories

#### 4.3.1 General

The following subsections provide a brief overview of some of the main contemporary criminological theories explaining common influencing factors that lead to people committing crime. By being aware of the different types of offenders and the different motivating factors influencing each type of offender, tailored security strategies can be implemented to specifically reduce the risks posed by each offender type.

#### 4.3.2 Neutralisation (Drift) Theory

Neutralisation theory strives to explain why some people drift in and out of delinquency. This Theory believes that people sense a moral obligation to be bound by law. This bind is in place most of the time, however when it is not, people will drift into delinquent behaviour.

The Theory states that delinquents hold values, beliefs and attitudes similar to those of ordinary citizens. However, they learn techniques which enable them to neutralise their behaviour, temporarily. This temporary neutralisation can therefore allow them to drift backwards and forwards between legitimate and illegitimate behaviours. These techniques act as defence mechanisms to release the delinquent from the restraints associated with the moral order.

A common reason a delinquent represses their dominant values is to avoid criticisms from their peers. This practice is commonly referred to as 'Peer Pressure'.

#### UoN NeW Space Implication

The Building security designs and strategies should strive to increase the perceived and actual risks of committing crime, increasing the time and effort needed to commit the crime, and reduce the rewards of committing the crime. Potential offenders influenced primarily by Neutralisation Theory motives, such as peer pressure, may be less likely to commit offences within the Building if the potential rewards are reduced, and the risk associated with committing crimes are increased compared to other locations. This potential outcome could be attributed to the fact that those influenced primarily by Neutralisation Theory motives, such as peer pressure may be more likely to deem the Building as an unattractive target due to it potentially being perceived as too difficult/risky, and therefore may choose not to commit crime within this area.

#### 4.3.3 Theory of Differential Association

The Theory of Differential Association is based on the social environment, the individuals in the environment and the values those individuals gain from the significant others in their environment.

The Theory of Differential Association views crime as a consequence of conflicting values. The Theory states that criminal behaviour is learned behaviour and is learned via social interaction with others. The process of learning criminal behaviour by association with criminal and anti-criminal patterns involves all of the mechanisms which are involved in any other learning.

## DRAFT

When criminal behaviour is learned, the learning includes both the techniques of committing the crime, which are sometimes very complicated, sometimes simple, and the specific direction of motives, drives, rationalisation and attitudes.

The specific direction of motives and drives is learned from the definitions of the legal code as favourable or unfavourable. A person becomes delinquent because of an excess of definitions favourable to violation of law over definitions unfavourable to violation of law. Individuals with an excess of criminal values will be more receptive to new criminal definitions (values) and less receptive to new non-criminal definitions.

### UoN NeW Space Implication

This type of offender is more difficult to protect against compared to one being influenced out of 'peer pressure', as they possess deeper conflicting values. This is due to the fact that they have essentially learned delinquent behaviour from the significant others (family, friends etc.) within their environment, and delinquent behaviour is regarded more as a 'social norm'.

Even though this type of offender is less likely to be influenced by the security strategies to be put in place throughout the UoN NeW Space area, a positive influence can still be achieved by increasing the perceived and actual risks of committing crime, increasing the time and effort needed to commit the crime and reducing the rewards of committing the crime within the UoN NeW Space area.

The Defence in Depth, and the Deter, Detect, Delay and Respond principles may also be effective at reducing the risks of crime posed by this type of offender. This is because they aren't reliant on a particular type of offender. So long as the series of barriers is effective in delaying the offender for long enough, and the detection function detects the offender early enough for a suitable response force to arrive in time, then the security treatment measures put in place should be more effective in protecting the Building against crime based risks.

#### 4.3.4 Strain Theory

Strain Theory says that crime is a social phenomenon. It is based on the understanding of individual and group behaviour, which sees crime as being shaped by wider social forces. Strain Theory states that crime does not occur because people are evil, but that crime is socially induced, and a criminal is a product of a specific social order.

This theory claims that the cause of crime is the presence of a social structure that holds out the same goals to all its members without giving them equal means to achieve them. It is this lack of integration between what the culture calls for and what the structure permits which causes deviant behaviour.

The Theory focuses on various acts of deviance which may be understood to lead to criminal behaviour.

### 5 Modes of Adapting to Strain

- Conformity - individuals accept both the goals and the prescribed methods for achieving them. Conformists will accept but not always achieve the goals of society.
- Innovation - individuals who accept societal goals but have few legitimate means to achieve them, thus they innovate their own means to get ahead, perhaps through robbery, embezzlement etc.
- Ritualism - individuals abandon the goals they once thought were within their reach and dedicate themselves to their current lifestyle. They play by the rules and have a safe daily routine.
- Retreatism - individuals who give up not only the goals but also the means. They often retreat into the world of alcoholism and drug addiction.
- Rebellion - individuals who reject the cultural goals and their legitimate means. They create their own goals and their own means by protest or revolutionary activity.

### Treatment Strategies:

Treatment strategies required in order to reduce the prevalence of this type of offender include enhancing the opportunities to reduce the strain on the individual – e.g. educational programs, employment projects, leisure outlets etc. A related treatment option is to re-socialise offenders so that their goals are more conventional and realistic.

# DRAFT

## UoN NeW Space Implication

This type of offender is also more difficult to protect against as the influences on the delinquent behaviour, and the effective treatment measures against this type of delinquent behaviour are wider social issues.

Even though this type of offender is less likely to be influenced by the security strategies to be put in place throughout the UoN NeW Space Building and surrounding areas, a positive influence can still be achieved by increasing the perceived and actual risks of committing crime in this area, increasing the time and effort needed to commit the crime and reducing the rewards of committing the crime within the Building and surrounding area.

The Defence in Depth, and the Deter, Detect, Delay and Respond principles may also be effective at reducing the risks of crime posed by this type of offender. This is because they aren't reliant on a particular type of offender. So long as the series of barriers is effective in delaying the offender for long enough, and the detection function detects the offender early enough for a suitable response force to arrive in time, then the security treatment measures put in place should be effective in protecting the Building against crime based risks.

The security treatment measures and CPTED principles employed at the UoN NeW Space Building may also displace crime committed by this and the other listed types of offenders by making the Building appear as a less desirable or more difficult/riskier target for their offending behaviour. Therefore these offenders may be more likely to target easier and less risky locations nearby, thereby displacing the crime from the UoN NeW Space Building location.

# DRAFT

## 5.0 Security Philosophies & Principles

### 5.1 General

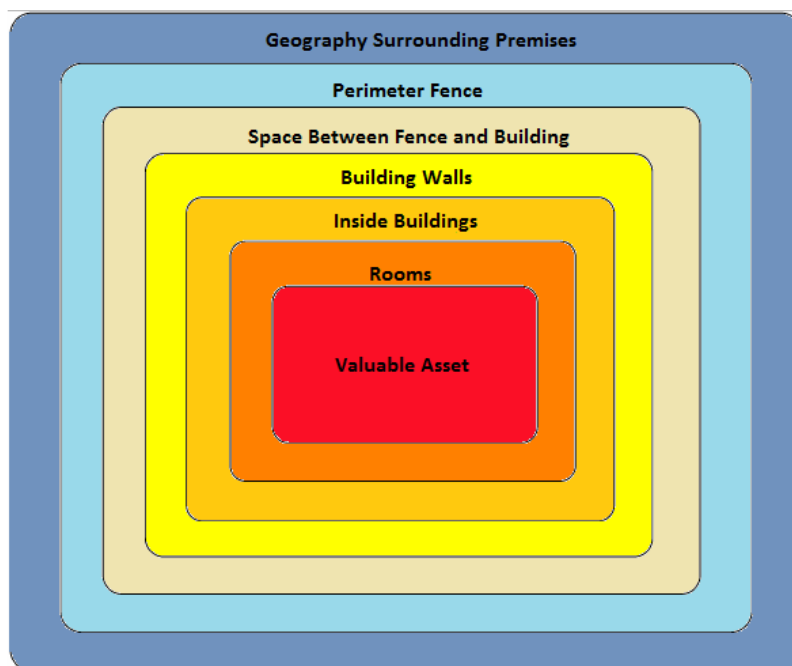
The security philosophies and principles outlined below form the basis of the security strategies and recommendations contained within this report.

### 5.2 Defence in Depth

The underlying purpose of physical security is to delay an intruder for a sufficient amount of time until an appropriate response group has arrived to apprehend the offender. This delay can best be achieved through a series of barriers instead of a single strong barrier. The Defence in Depth security principle imposes a succession of barriers, which require access, between the public and the asset.

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

Figure 1 Defence in Depth



The Defence in Depth principle should be used in conjunction with the D<sup>3</sup>R security principle outlined in Section 5.3.

#### 5.2.1 Outer Layer

Physical controls at the outer protective layer or perimeter may consist of fencing or other barriers, protective lighting, signs, and intrusion detection systems. 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 generally 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 also provides the earliest opportunity for detection and identification of intrusions.

#### 5.2.2 Middle Layer

The middle layer, at the exterior of buildings on the site, may consist of protective lighting, intrusion detection systems, locks, bars on doors and windows, signs, and barriers such as fencing and the façade of the building itself.



# DRAFT

Protection of skylights, ventilation ducts and other miscellaneous openings should also be considered, depending on the risk profile of the site. Walls and openings (such as air intake vents) on the sides of buildings should also be examined for vulnerability to penetration. Intrusion detection at the building perimeter increases the effectiveness of security or police response.

## 5.2.3 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 are normal at this layer: window and door bars, locks, barriers, signs, intrusion detection systems, and protective lighting.

The value of an asset being protected affects the amount of protection required. A high value asset housed in an inner area might require signs defining access requirements for the area, specifically reinforced walls, a structurally reinforced door with high security locks/electronic access control/biometric lock, intrusion detection systems, video surveillance to monitor access, and safes and vaults to house the asset itself.

## 5.3 Deter, Detect, Delay & Respond (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.

### 5.3.1 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, CCTV coverage and open plan designs (where practical) can deter opportunistic crime from occurring. Security patrols could also be considered in order to deter crime from occurring at the UoN NeW Space site.

### 5.3.2 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 can be achieved by installing and using passive infrared (PIR) volumetric detectors in nominated buildings, and installing and monitoring CCTV. By ensuring each site has appropriate illumination levels and has clear sight lines and natural surveillance where practical, can also significantly improve the ability to provide the detection function. Security patrols could also be considered in order to detect crime/unauthorised access.

### 5.3.3 Delay

When unauthorised access to a restricted space 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 fences, locks, safes, 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 site with the asset.

### 5.3.4 Response

A timely and appropriate response is required at the UoN NeW Space site by Security guards, or the local Police, depending on the nature of the event.

## 5.4 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 UoN NeW Space site are the use of;

- High security fencing where appropriate;
- High security locks and keying systems where required;
- Specific construction methods for perimeter doors, door frames and windows;

## DRAFT

- Limiting miscellaneous openings on building perimeters and treating any large openings with security grilles, tamper resistant fasteners etc.;
- Electronic detection and access control systems; and
- CCTV coverage of specific areas.

### 5.5 Situational Crime Prevention

Situational crime prevention is based on the theory that crime is the result of opportunities to commit crime and can be prevented by reducing these opportunities. These opportunities can be reduced by increasing the perceived and actual risks of committing the crime, increasing the effort needed to commit the crime and reducing the rewards of committing the crime.

UoN should incorporate the situational crime prevention theory into future security policies, procedures, specifications and designs. In order to increase the perceived and actual risks, UoN can implement a number of measures including ensuring the Building and precinct layouts enhance natural surveillance, provide CCTV coverage to capture any security incidents with sufficient detail and install security signage to promote territorial reinforcement. In order to increase the effort and to protect the safety of UoN staff, contractors and students, quality security measures such as high security locks and keys should be implemented to satisfy legislative requirements for providing a safe and secure workplace.

UoN can reduce the rewards of committing crime by minimising the amount of assets with high monetary value (cash/ATM's, computers, etc.) that they have on site and ensuring that they are secured appropriately through a combination of physical, electronic and procedural security elements.

# DRAFT

## 6.0 Security Risk Management

### 6.1 Overview

The purpose of risk management is to identify, quantify, and prioritise risks against criteria for risk acceptance and objectives relevant to the organisation (in this case UoN). 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 assessments should 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 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 Building;
- Improve the identification of opportunities and threats;
- Achieve compatible risk management practices between Facilities;
- 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 UoN NeW Space Building and surrounding areas, or within a specific area, project or activity;
- Those responsible for developing risk management policy within their organisation, and the Building;
- Those who need to evaluate an organisations/Buildings 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.

# DRAFT

## 6.2 Principles

For risk management to be effective within the Building and UoN Campus, UoN should strive 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 UoN. Risk management is part of the responsibilities of management and an integral part of all organisational 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 University's 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 University's and the Faculty of Business and Laws' objectives.

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

Appropriate and timely involvement of stakeholders and, in particular, decision makers at all levels of the UoN hierarchy, 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.

# DRAFT

## 6.3 Framework

### 6.3.1 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.

## 6.4 Mandate and Commitment

The introduction of risk management and ensuring its ongoing effectiveness require strong and sustained commitment by management of the organisation, as well as strategic and rigorous planning to achieve commitment at all levels. Where appropriate, UoN 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;
- 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.

## 6.5 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;

# DRAFT

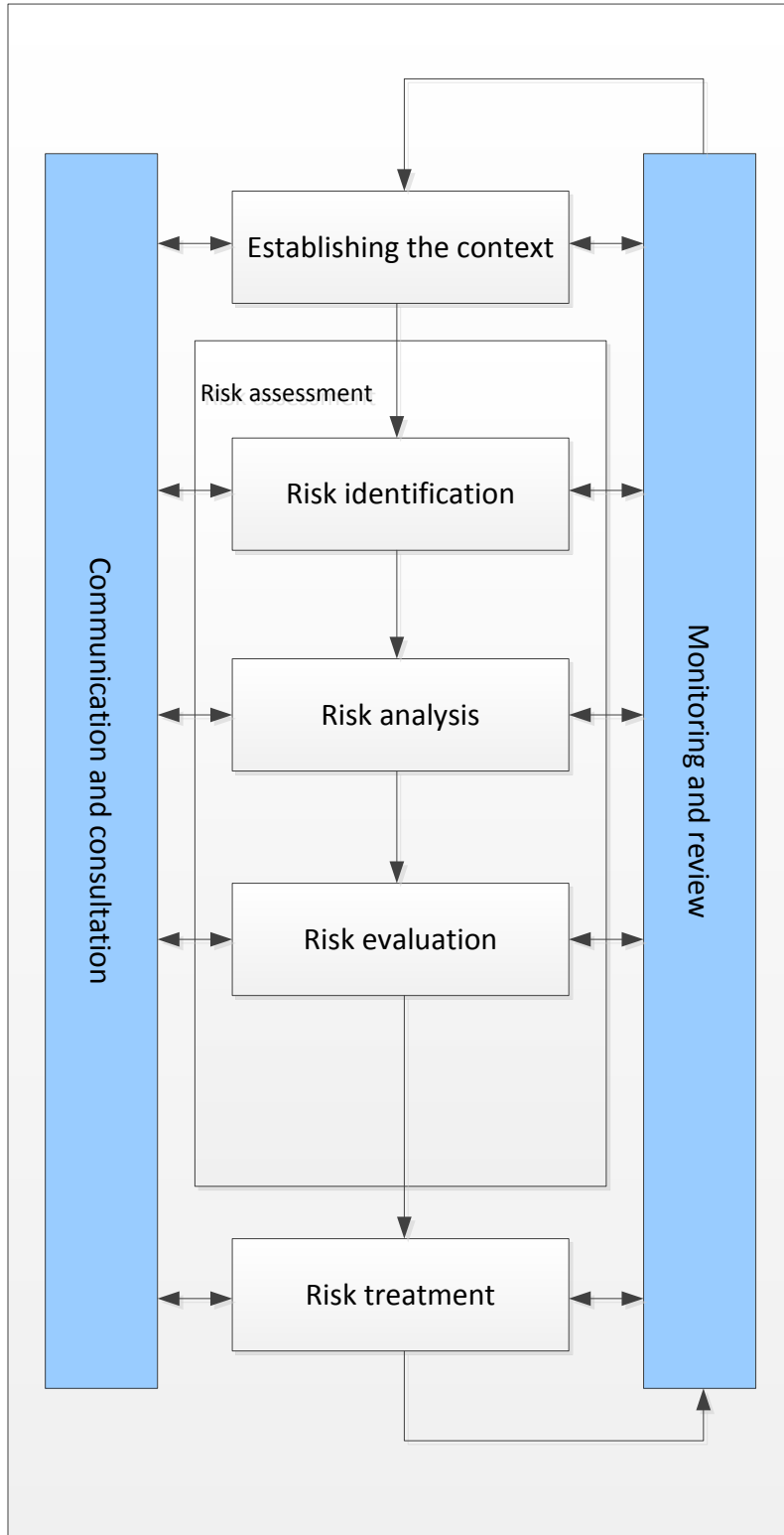


Figure 2 ISO 31000 Risk Management Process

# DRAFT

## 7.0 Security Risk Assessment

### 7.1 Communication & Consultation

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

### 7.2 Context Establishment

#### 7.2.1 External Context

The term 'external context' refers to gaining an understanding of the external environment in which the UoN NeW Space Building, the Faculty of Business and Law, and the University of Newcastle is operating or may be operating in the future. In assessing the external context, the key objective is to identify and characterise factors in the external environment that are going to have an effect on the Building/Faculty/University. Ultimately, the focus will be on those factors which will either directly or indirectly have security risk implications for the Building/Faculty/University. 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 Building/Faculty/University is operating, this report will examine;

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

#### Suburb Profile

The University of Newcastle NeW Space building is located within the suburb of Newcastle.

As of the 2011 Australian Government Census, the suburb of Newcastle has a population of 2,384. The suburb essentially comprises the Newcastle CBD.

Based on information collected during the 2011 Census, Newcastle is largely an Australian born, English only speaking, and Christian suburb. Newcastle has an above average community hailing from the USA, with over three times the NSW average, and is also above the NSW average for people identifying themselves as following no religion.

Newcastle has a slightly above average number of residents who are employed full time, but is slightly below average when it comes to residents employed part time. The unemployment rate in Newcastle is slightly below the NSW average at 5.6% compared to 5.9%. The median incomes in Newcastle are above the NSW average in all three categories.

The main occupation type within Newcastle is Professionals, followed by Managers and Clerical and Administrative Workers. Newcastle has an above average number of Professionals (39.8% compared to state average of 22.7%), and Managers (15.1% compared to 13.3%). The number of residents employed in the other main employment categories is below the state averages.

Newcastle is a high density suburb with 86.7% of dwellings either flats, units or apartments. The NSW state average for these dwelling types is 18.8%. The majority of Newcastle dwellings are rented, with 54.1% of residents renting, compared to the NSW average of 30.1%.

Table 1 Population Profile – Newcastle

Indicator	Percentage	NSW Average
Population	2,384 (Total)	N/A

**DRAFT**

Males	52.5%	49.3%
Females	47.5%	50.7%
Australian Born	72.2%	68.6%
Overseas Born	27.8%	31.4%
Indigenous Australian	1.5%	2.5%
<b>Age Structure</b>		
Median Age	34	38
Aged 0-14 years	6.4%	19.2%
15-29 years	33.5%	19.7%
30-44 years	21.6%	20.9%
45-64 years	25.6%	25.5%
Aged 65+	12.8%	14.7%
<b>Birth Place</b>		
Australia	72.2%	68.6%
England	2.5%	3.3%
New Zealand	1.9%	1.7%
United States of America	1.3%	0.4%
China	1.9%	2.3%
India	0.8%	1.4%
Total Overseas Born	21.6%	31.4%
<b>Religion</b>		
No Religion	28.6%	17.9%
Catholic	21.8%	27.5%
Anglican	20.2%	19.9%
Uniting Church	5.8%	3.9%
Presbyterian and Reformed	2.8%	3.1%
<b>Language</b>		
English Speaking Only	80.1%	72.5%
Mandarin	1.3%	2.0%
Arabic	1.1%	2.7%
Persian (excluding Dari)	0.8%	0.2%
German	0.7%	0.3%
Italian	0.7%	1.2%

**Political Context**

The suburb of Newcastle falls within the City of Newcastle Local Government Area (LGA), the State Electorate of Newcastle, and the Federal Division of Newcastle.



# DRAFT

Currently the State Electorate of Newcastle is held by the Liberal Party of Australia. Historically, Newcastle has been held either by the Australian Labor Party or by Independents. This is the first time either the state or federal electorates have been held by the Liberal Party of Australia.

Currently the Federal Division of Newcastle is held by the Australian Labor Party. The Division has also always been held by the Australian Labor Party.

**Table 2** Socio-Economic Context

Indicator	Percentage	NSW Average
<b>Employment Status</b>		
Employed – Full Time	66.2%	60.2%
Employed – Part Time	24.1%	28.2%
Away From Work	4.1%	5.7%
Unemployed	5.6%	5.9%
<b>Occupation</b>		
Professionals	39.8%	22.7%
Managers	15.1%	13.3%
Clerical & Administrative Workers	12.1%	15.1%
Technicians & Trade Workers	8.8%	13.2%
Sales Workers	8.7%	9.3%
Community & Personal Services Workers	8.4%	9.5%
Labourers	3.7%	8.7%
Machinery Operators & Drivers	2.2%	6.4%
<b>Median Income (Weekly)</b>		
Personal	\$940	\$561
Family	\$2,173	\$1,477
Household	\$1,750	\$1,237
<b>Housing Tenure</b>		
Owned	23.1%	33.2%
Owned with a Mortgage	21.0%	33.4%
Renting	54.1%	30.1%
<b>Dwelling Structure</b>		
Separate House	5.4%	69.5%
Semi-Detached, row or terrace house, townhouse etc	5.8%	10.7%
Flat, unit, apartment	86.7%	18.8%
Other Dwelling	2.0%	0.9%
Total Occupied Private Dwellings	78.4%	90.3%
Total Unoccupied Dwellings	21.6%	9.7%

# DRAFT

## Market Context

The suburb of Newcastle comprises a mix of commercial, residential and education facilities. The suburb of Newcastle comprises the Newcastle Central Business District.

## Infrastructure Context

The key infrastructure nearby the University of Newcastle includes;

- Newcastle City Council;
- Civic Theatre;
- Civic Park;
- Civic Station; and
- Newcastle Museum.

## Social Infrastructure Context

### *Emergency Services*

NSW Police: The University of Newcastle is located within the Newcastle City Local Area Command (LAC), within the Northern Region.

Newcastle Police Station is a 24 hour police station, and is located approximately 1.4km from the University, enabling them to provide a quick and timely response during emergency situations at the University.

### Fire and Rescue NSW:

Newcastle Fire Station is located approximately 550m from the University, enabling them to provide a quick and timely response during emergency situations at the University.

### Medical Services

James Fletcher Hospital is located approximately 1.5km from the University.

Lingard Private Hospital is located approximately 2.2km from the University.

## 7.2.2 Internal Context

The University of Newcastle (UoN) is one of Australia's most innovative regional universities, ranked in the top 3% of universities worldwide; and in the top 10 Australian universities. The UoN is committed to the highest possible standards in teaching, learning and research; to the pursuit of quality; and strives to further improve its results in all aspects of higher education.

The UoN has secured funds from Commonwealth and State Governments to assist the UoN in the construction of the NeW Space project. This comprises a new building on a prominent site at the corner of Auckland and Hunter streets in Newcastle, and alterations to University House.

The project will accommodate the offices and teaching accommodation for the Faculty of Business and Law. The facility will contain a Library and Learning Hub to support Business and Law students and Music students from the nearby Newcastle Conservatorium of Music. The new Library and Learning Hub will also provide support to any UoN students who wish to use it and it is particularly directed at those students living in the central city area.

Fully developed, the NeW Space facility will support face to face teaching for over 3,000 undergraduate (UG) students, many hundreds of post-graduates (PG) and over 300 staff.

## 7.3 Risk Identification

### 7.3.1 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.

# DRAFT

## 7.3.2 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 Local Government Area within which the University and UoN NeW Space Building 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.

## 7.3.3 Sources of Threat

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).

The likely sources of threats that the UoN Building may be exposed to include;

- Trespassers;
- Vandals;
- Graffiti Artists (Taggers);
- People under the influence of drugs/alcohol;
- Antisocial people;
- Criminals;
- Issue motivated groups;
- Disgruntled students, staff, contractors, members of the public;
- Former students/staff/contractors; and
- People suffering from a mental health condition.

## 7.3.4 Most Prevalent Crimes

The following is a list of the most prevalent crimes to occur in the City of Newcastle LGA during 2012 that are relevant to the University. Also listed are the total offences for each offence type and the rank (out of 140) compared to the other LGA's (the higher the rank, the lower the crime levels – i.e. a rank of 1 means the LGA has the highest incidence of that crime, whereas a rank of 140 means the LGA has the lowest incidence of that crime):

- Malicious damage to property (2,651 offences, #32);
- Steal from a motor vehicle (1,746 offences, #9);
- Assault – non-domestic violence related (1,232 offences, #17);
- Theft (1,164 offences, #13);
- Fraud (1,125 offences, #15);
- Harassment, threatening behaviour and private nuisance (787 offences, #49);
- Motor vehicle theft (667 offences, #8);
- Break and enter non-dwelling (573 offences, #42);
- Liquor Offences (378 offences, #44);
- Offensive Conduct (349 offences, #27);
- Sexual or Indecent Assault (313 offences, #46);
- Possession and/or use of cannabis (307 offences, #85);

## DRAFT

- Steal from Person (292 offences, #5);
- Trespass (206 offences, #75);
- Prohibited and regulated weapons offences (196 offences, #69);
- Arson (193 offences, #53);
- Robbery (187 offences, #6);
- Offensive Language (164 offences, #43); and
- Possession and/or use of amphetamines (164 offences).

Refer to Appendix C for a more detailed list of offences.

### 7.3.5 Highest Ranking Crimes

The following is a list of the offence types that the City of Newcastle LGA ranks highly in when the incidence rate is compared against the other LGA's:

1. Steal from Person (292 offences, #5);
2. Robbery (187 offences, #6);
3. Motor vehicle theft (667 offences, #8);
4. Steal from a motor vehicle (1,746 offences, #9);
5. Theft (1,164 offences, #13);
6. Fraud (1,125 offences, #15);
7. Assault – non-domestic violence related (#17);
8. Offensive Conduct (349 offences, #27);
9. Malicious damage to property (2,651 offences, #32);
10. Break and enter non-dwelling (573 offences, #42);
11. Offensive Language (164 offences, #43);
12. Liquor Offences (378 offences, #44);
13. Sexual or Indecent Assault (313 offences, #46); and
14. Harassment, threatening behaviour and private nuisance (787 offences, #49).

# DRAFT

## 7.3.6 City of Newcastle LGA Crime Hotspot Map

The map below portrays the assault crime hotspots for the City of Newcastle LGA:

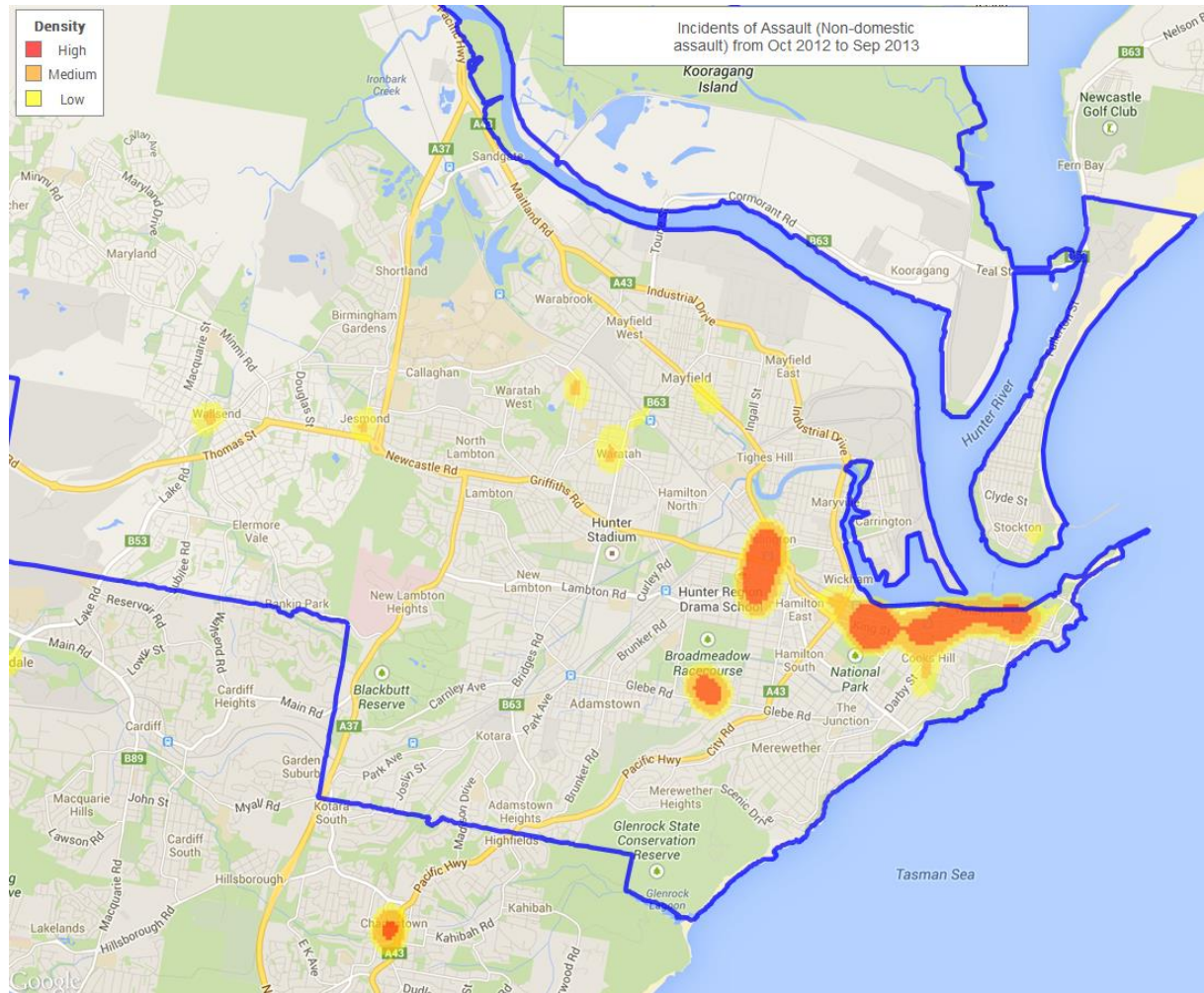


Figure 3 City of Newcastle Crime Hotspot Map

## 7.3.7 Crime Analysis

As can be observed in the rankings for each offence type above, the City of Newcastle LGA has generally high to mid-levels of crime across the most prevalent offence categories. In particular the City of Newcastle LGA ranks in the top 10 for steal from person, robbery, steal motor vehicle, and steal from motor vehicle.

As can be seen in the 5 year trend table below, 6 of the 10 most prevalent crimes applicable to the University and UoN NeW Space Building have either been stable over this period or have a negative average annual change in occurrence. Based on these trends, the likelihood of these offences occurring in the future should either remain the same as currently assessed, or reduce.

**DRAFT****Table 3 5 Year Trend – Top 10 Offences**

Offence	Jan-Dec 2008	Jan-Dec 2009	Jan-Dec 2010	Jan-Dec 2011	Jan-Dec 2012	60 Month Trend	Ave Annual % Change
Malicious damage to property	3,838	3,484	3,179	3,121	2,651	Down	-8.8%
Steal from motor vehicle	2,399	1,829	1,872	2,212	1,746	Down	-7.6%
Assault – non-domestic violence related	1,355	1,349	1,439	1,260	1,232	Down	-2.4%
Theft	1,232	1,127	1,150	1,125	1,164	Stable	Stable
Fraud	901	810	1,007	1,072	1,125	Up	5.7%
Harassment, threatening behaviour and public nuisance	512	500	555	646	787	Up	11.3%
Motor vehicle theft	930	812	751	758	667	Down	-8.0%
Break and enter non-dwelling	1,104	772	562	594	573	Down	-15.1%
Liquor Offences	320	289	317	339	378	Up	11.5%
Offensive Conduct	413	300	296	307	349	Up	13.7%

**Table 4 Rising Offences – All Offences**

Offence	Jan-Dec 2008	Jan-Dec 2009	Jan-Dec 2010	Jan-Dec 2011	Jan-Dec 2012	60 Month Trend	Ave Annual % Change
Possession and/or use of other drugs	31	33	44	53	73	Up	23.9%
Breach bail conditions	417	369	459	739	962	Up	23.2%
Possession and/or use of amphetamines	95	53	81	106	164	Up	14.6%
Offensive Conduct	413	300	296	307	349	Up	13.7%
Liquor Offences	320	289	317	339	378	Up	11.5%

**DRAFT**

Harassment, threatening behaviour and public nuisance	512	500	555	646	787	Up	11.3%
Other Offences	262	286	325	262	356	Up	8.0%
Fraud	901	810	1,007	1,072	1,125	Up	5.7%
Possession and/or use of cannabis	259	222	315	293	307	Up	4.3%

**7.4 Risk Assessment****7.4.1 Process**

The security risk assessment process involved a desktop analysis of the relevant NSW Bureau of Crime Statistics and Research crime statistics for the Local Government Area of City of Newcastle, within which the University and NeW Space Building is located. This information is used to develop a risk profile for the Building which allows likelihood and consequence values to be assigned to identified individual threat sources. This assessment is documented in the Risk Matrix (refer to Appendix A).

The identified risks are ranked from Low to High, with Low risks to be monitored for change. Any risks that fall within the categories of Medium to High 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 UoN stakeholders.

**7.4.2 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 5 Likelihood Definitions**

<b>Likelihood</b>	<b>Almost Certain</b>	<b>Over 99% probability, or Happens often, or Could occur within days to weeks</b>
	<b>Likely</b>	<b>&gt;50% probability, or Could easily happen, or Could occur within a year or so</b>
	<b>Possible</b>	<b>&gt;10% probability, or Could happen/Has occurred before, or could occur within a year or so</b>
	<b>Unlikely</b>	<b>&gt;1% probability, or Has not happened yet, but could, or Could occur after several years</b>
	<b>Rare</b>	<b>&lt;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.</b>

**Table 6 Consequence Definitions**

**DRAFT**

		People	Property & Equipment	Business Operations	Information	Reputation
Consequence	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 sensitive to international matters.	Royal Commission, Parliamentary inquiry or sustained adverse national/international media
	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 Federal Government and national matters	Intense public, political and media scrutiny. Eg: front page headlines, TV, etc
	Moderate	Major or Serious injury to staff (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 UoN, intellectual property or operations.	Strong scrutiny by external committees or agencies
	Minor	Minor Injury to staff or visitors (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 UoN interests.	Internal scrutiny by executive, 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 7 Risk Rating Matrix and Definitions

		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	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 UoN New Space.

In the context of the UoN New Space project, this risk assessment extends primarily to the personal safety of staff, students and visitors. It also considers the risk, loss or compromise of University/ UoN New Space 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 University/Faculty and diminished reputation;
- Negative impacts on University/Faculty/UoN New Space objectives;



## DRAFT

- Partial or full disruption of University/Faculty/UoN New Space 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/students/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 Newcastle City LGA. These statistics are not detailed to suburb or street level and therefore they may not provide a complete representation of historic incidents at the University.

### 7.4.3 Security Risks

The risk events listed in the tables below are assessed as having High to Medium 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 8 High to Medium Risks**

Risks	How It Can Be Realised	Risk Rating (Pre-treatment)	Risk Rating (Post-treatment)
Targeted Theft	Theft of property, equipment or information resulting in financial loss to the Building/Faculty/University, cessation or interruption to services, loss of personal property, embarrassment or impact to reputation, etc	High	Medium
Theft - Opportunist	Theft of equipment/assets from theatres/library/teaching spaces/student hub/offices etc	High	Medium
Drug/Alcohol offences	Intoxicated persons posing a risk to themselves or others	High	Medium
Robbery	Of students/staff/contractors/general public	Medium	Medium
Harassment, threatening behaviour and private nuisance	Of students/staff/contractors/general public	Medium	Medium
Physical assault	Of students/staff/contractors/general public	Medium	Medium
Vandalism/graffiti	General by criminals, opportunists, youths, gangs etc	Medium	Medium
Forced Access - Pedestrian (Break and Enter)	Forced pedestrian access or entry to the Building areas resulting in possible theft, vandalism or sabotage to equipment, harm to staff, etc.	Medium	Medium
Sexual Assault	Of students/staff/contractors/general public	Medium	Medium
Compromise of university/faculty information	Inappropriate management and storage of security related information	Medium	Medium

# DRAFT

## 7.5 Threat Assessment

### 7.5.1 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.

### 7.5.2 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 al-Qaeda, role of international criminal and terrorist groups 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
Influence 3rd party decisions	Vengeance
Seek vengeance	Punishment for perceived societal wrongs
Seek self-justification	Proxy atonement
Pathological disorders	Influence change

### 7.5.3 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.

### 7.5.4 Measuring the Threat

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

# DRAFT

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

## 7.6 Risk Analysis

### 7.6.1 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

#### Risk Rating: Medium

Trespass has been rated as Medium based on the possible frequency of occurrence, of both inadvertent and deliberate trespass.

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

- Break and Enter (non-dwelling);
- Unauthorised Building entry/egress; and
- Unauthorised access to restricted areas.

Based on the BOSCAR stats for the City of Newcastle LGA, those most likely to conduct break and entering (non-dwelling) are males aged 30-39 or 10-17 years old. The main premises type targeted by these offenders is Retail/Wholesale premises, followed by Education premises. Break and entering (non-dwelling) offences are most likely to occur on Monday and Friday mornings between the hours of 12-6am, and least likely to occur between the hours of 6am – 12pm on a Thursday or Friday. Only 2.4% of break and entering (non-dwelling) offences were alcohol related.

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

# DRAFT

In order to treat the risks posed by unauthorised access into the Building and its restricted areas, a clear delineation between public and restricted space should be achieved. Physical barriers should be installed where practical to reduce the opportunity for trespass. Signage should be installed where appropriate notifying persons of restricted space, dangerous space (plant/switch rooms etc) and that security measures are in place (eg. CCTV signage). Roaming patrols by the on-site security officers can provide both a deterrence to trespass type offences and a response to incidences.

## 7.6.2 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

#### Risk Rating: High to Medium

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 Medium risks (pre-treatments), and as Medium risks (post treatment).

Anti-social behaviour, such as loitering and harassment are a concern for staff/contractors, students, and the general public. The risk assessment identified these risks as High to Medium due to the high likelihood of occurrence.

While the consequence of this type of risk does not directly impact on the ability for the University to provide education services, it does negatively contribute to the student experience and a reduction in the reputation of the University of being able to offer a safe and secure environment for its users. Consequently, this risk needs to be carefully managed to ensure that the University is seen to be doing everything possible towards creating a safe environment for its students, staff and the general public. Electronic security measures can be implemented to deter persons from loitering around the Building. These can include CCTV as deterrence, and to provide recorded video images that may be used for prosecution and conviction purposes. In addition, physical security measures should be provided to ensure the Building perimeter can remain secure. Security signage can be used to provide a clear boundary between public and private areas can be installed. Staff should also be aware of response procedures to anti-social behaviour such as loitering or harassment by drug affected persons.

CPTED recommendations, including clear sight lines and low level barriers should be implemented to provide natural surveillance of intoxicated or anti-social people. Lighting can be used to enhance natural and electronic surveillance, provide a deterrence, and to assist natural access control. Emergency Help Points will be installed

# DRAFT

for the general public to call for assistance during emergency situations. Fixed duress alarms should be provided for staff/contractors (working in high risk areas (eg client facing areas). Reporting and response procedures should be produced for staff.

### 7.6.3 Risk Trend: Vandalism

#### Threat posed by Vandalism

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

#### Threat Analysis

Vandals have been assessed as having Expressed Intent, due to the fact that high value items are likely to be stored within the Building.

Vandals 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

##### Risk Rating: Medium to Low

The risk trend of vandalism includes graffiti and malicious damage to the Building and University infrastructure. The risk of vandalism has been given a risk rating of Medium to Low due to the frequent likelihood of occurrence and the generally insignificant consequences.

Based on the BOSCAR stats for the City of Newcastle LGA, those most likely to conduct malicious damage to property are males aged 20-29 years old. Malicious damage to property offences are most likely to occur during the hours of 12-6am on a Sunday, and least likely to occur during the hours of 12-6am on a Tuesday. Only 10.18% of malicious damage to property offences is alcohol related.

Education type premises are the 4<sup>th</sup> most likely premises type within the City of Newcastle LGA to be victim of malicious damage to property. However, this only equates to 5.6% of the recorded incidences of malicious damage to property within the City of Newcastle during 2012.

The recommended treatment measures that can be incorporated in order to lower the risk of vandalism include:

- Adequate security lighting to provide deterrence through improved chance of detection and increased perception of detection of criminal behaviour in and around the Building;
- CCTV surveillance and security signage to provide deterrence to criminal behaviour, and to provide recorded footage that can be used for post-event analysis and potentially for identification and prosecution purposes;
- The implementation of CPTED recommendations including clear sight lines and good natural surveillance to assist detection of criminal behaviour;
- The timely repair of damage/graffiti to enhance the territorial reinforcement aspects of the site; and

# DRAFT

- Adequate physical and electronic security measures to restrict access to the Building.

## 7.6.4 Risk Trend: Theft & Robbery

### Threat posed by Theft

		<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	<b>Significant</b>	High
	<b>Low</b>	Low	Medium	Significant

### Threat Analysis

Thieves have been assessed as having Expressed Intent, due to the fact that high value items are likely to be stored within the Building.

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

#### Risk Rating: High to Medium

Theft and robbery type security risks have been rated as High to Medium risks based on the likely frequency of occurrence, and the fact that the LGA ranks highly for these offence types.

Based on the BOSCAR stats for the City of Newcastle LGA, those most likely to conduct robbery and steal from person offences are males aged 10-17 years old, while those most likely to be the victims of robbery are males aged 18-29 years old, and those most likely to be victims of steal from person offences are females aged 18-29 years old.

Robbery offences within the City of Newcastle LGA are most likely to occur between 12pm and 6pm on a Saturday or 6am and 12pm on a Tuesday, and least likely to occur on a Wednesday during the hours of 6am and 12pm, or Thursday during the hours of 12 – 6pm. Robberies within the City of Newcastle LGA are most likely to occur in an Outdoor/Public Place, followed by a Retail/Wholesale place. Education type premises only had 2 recorded incidents during 2012. 22.6% of robbery offences are alcohol related.

Steal from person type offences are most likely to occur within licensed premises or Outdoor/public spaces, with Education premises only have 13 recorded incidences. However, despite licensed premises being the most common place for steal from person type offences occurring, only 8.9% of these offences are alcohol related.

Saturdays and Sundays are the most likely days for steal from person type offences to occur, especially during the hours of 12-6pm on Saturday through to 12-6am on a Sunday. Monday to Wednesday mornings from 12-6am, and Fridays from 6am – 12pm are the least likely times for steal from person type offences to occur within the City of Newcastle LGA.

Based on the BOSCAR stats for the City of Newcastle LGA, those most likely to conduct motor vehicle theft are males aged 10-17 years old. Motor vehicle theft is most likely to occur at Outdoor/Public Place, followed by Residential type premises. Only 2 reported motor vehicle theft within the City of Newcastle LGA during 2012 occurred at a Public Transport type premises.

Based on the BOSCAR stats for the City of Newcastle LGA, those most likely to conduct steal from motor vehicle are males aged 20-29 years old. Steal from motor vehicle type offences are most likely to occur at Outdoor/Public

# DRAFT

Place, followed by residential type premises. Only 13 reported steal from motor vehicle type offences within the City of Newcastle LGA during 2012 occurred at an Education type premises.

Security treatment measures that can be implemented to help lower the risks posed by theft and robbery type offences include:

- Security lighting, CCTV surveillance and security signage to provide deterrence to criminal behaviour.
- Implement CPTED recommendations including clear sight lines, good natural surveillance, natural access control and territorial reinforcement.
- Adequate electronic and physical security to prevent unauthorised access to the Building and its surrounding areas and assets.
- Install intruder alarm system to monitor the integrity of the Building and restricted areas.

## 7.6.5 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/visitors/students/general public 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/visitors/students/general public 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

#### Risk Rating: Medium

- Assault – non-domestic violence related (1,232 offences, #17);

Non-domestic violence related assault is the third most prevalent offence type within the City of Newcastle LGA, and has been rated as a Medium risk.

Based on the BOSCAR stats for the City of Newcastle LGA, those most likely to conduct non-domestic violence related assault are males aged 20-29 years old. Those most likely to be the victims of non-domestic violence related assault are males aged 18-29 years old.

Non-domestic violence related assault within the City of Newcastle LGA is most likely to occur during the hours of 6pm Saturday, and 6am Sunday. Within those timeslots the 12-6am timeslot on a Sunday is the worst for non-domestic violence related assault. Non-domestic violence related assault is least likely to occur between 12-6am on a Monday, Tuesday or Wednesday.

46% of non-domestic violence related assaults within the City of Newcastle are alcohol related, while only 1.8% of non-domestic violence related assault occurred at Education type premises within the City of Newcastle during 2012.

# DRAFT

Security treatment measures that can be implemented to help lower the risks posed by assault include:

- Security lighting, CCTV surveillance and security signage to provide deterrence to criminal behaviour.
- Implement CPTED recommendations including clear sight lines, good natural surveillance, natural access control and territorial reinforcement.
- Adequate electronic and physical security to prevent unauthorised access to the Building and restricted areas.
- The provision of Emergency Help Points for students to call for assistance during emergency situations.
- The provision of fixed duress alarms for staff, particularly those in customer facing roles/areas.

### 7.6.6 Risk Trend: Drug and Alcohol Related Offences

#### Risk Rating: High

Drug and alcohol related offences have been rated as high risks, based on their potential likelihood of occurrence.

Possession and/or use of cannabis is the 12<sup>th</sup> most prevalent offence type in the LGA, while liquor offences are the 9<sup>th</sup>. Possession and use of other drugs has a 60 month average annual increase of 23.9%, possession and/or use of amphetamines has 60 month average annual increase of 14.6%, liquor offences have a 60 month average annual increase of 11.5%, and possession and use of cannabis has a 60 month average annual increase of 4.3%.

#### UoN NeW Space Analysis

The risk of antisocial behaviour – drug and alcohol related incidents have been rated as High.

A continued upward trend in the incidence of amphetamine/alcohol and other drug use may increase the risks associated with non-domestic violence related assault, antisocial behaviour including harassment and threatening behaviour, malicious damage to property, and theft and robbery (in order to fund the habit).

In order to reduce the risks associated with drug and alcohol related incidents, the following treatment measures are recommended;

- 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 recommendations, including clear sight lines and low level barriers to provide natural surveillance of intoxicated or anti-social people.
- Install Help Points and provide staff/contractors with duress alarms where necessary.
- Produce reporting and response procedures for University staff.
- Security lighting, CCTV surveillance and clear sightlines are likely to provide deterrence and displace any dealing of drugs to other areas instead of the Building or University.

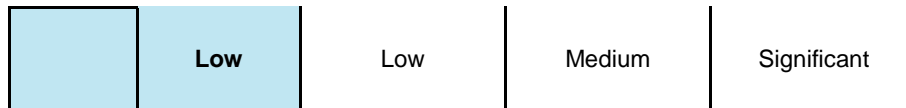
### 7.6.7 Risk Trend: Terrorist Type Activities & Active Shooters

#### 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	<b>High</b>



# DRAFT



## 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

### Risk Rating: Medium

As can be observed in the Appendix A and the table above, terrorist based security risks and active shooters pose a risk to the University. 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 UoN NeW Space Building, and the historical occurrence of these types of events taking place in education settings within Australia and internationally. Due to the incidence of active shooters within Education type premises (very rare in Australia, but common in some countries overseas), this risk has been examined.

The National Terrorism Public Alert level is currently (as at the date of this report) **Medium**.

The National Terrorism Public Alert System is a range of four levels that communicate an assessed risk of terrorist threat to Australia. The four levels are:

- **Low** - Terrorist attack is not expected;
- **Medium** – Terrorist attack could occur;
- **High** – Terrorist attack is likely; and
- **Extreme** – Terrorist attack is imminent or has occurred.

The National Terrorism Public Alert 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.

Australia has been at a 'Medium' level of alert since the four levels of national terrorism alert were introduced in 2003.

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 Al-Qa'ida 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;

- 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.

# DRAFT

- Building 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.
- CCTV & security lighting to provide deterrence, surveillance and detection of suspicious objects/activity.
- Natural surveillance strategies to be implemented at the Building and its surrounding areas 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 throughout the Building.
- Standoff distances to be provided through natural and physical access control measures where practical.
- 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, education campuses, sporting venues, shopping and business precincts, tourism/entertainment venues/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.

## 7.7 Risk Evaluation

### 7.7.1 General

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

### 7.7.2 Tolerance of Risk

Decisions on the tolerability of risk for UoN NeW Space has based upon the ALARP approach ('As Low as Reasonably Practical', Figure below). This approach recognises the concept of a gradient of tolerability but divides the gradient up into three broad bands based upon a:

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

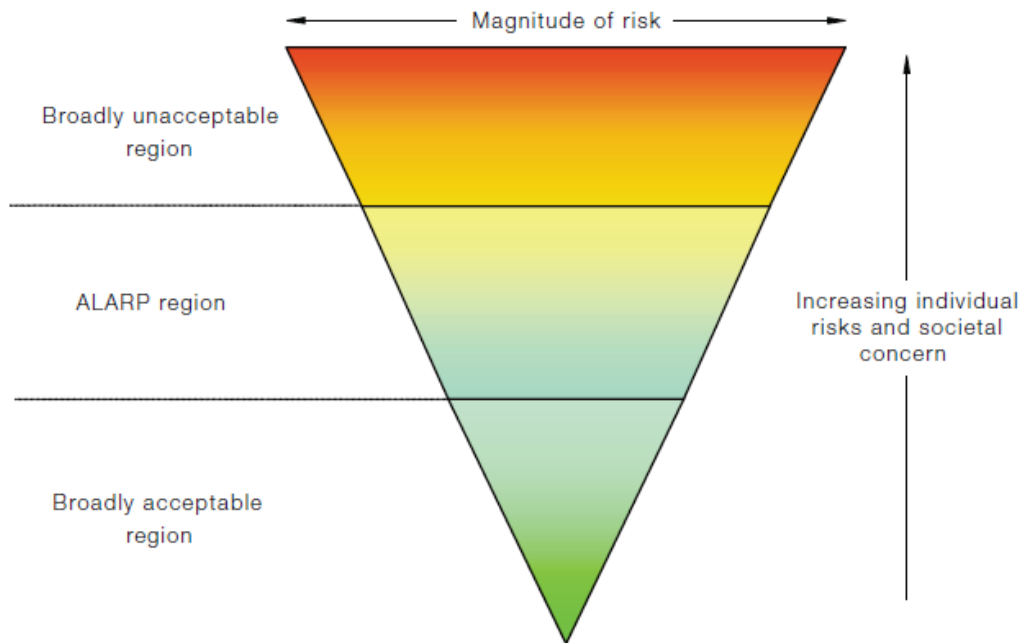
**DRAFT**

Figure 4 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.

## **7.8 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 (eg. Insurance, contracts etc); and
- Retaining the risk by informed decision.

Refer to Section 8.0 for the risk treatment recommendations.

Refer to Appendix B for the Security Treatment Matrix.

# DRAFT

## 7.9 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 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.

### 7.9.1 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

## DRAFT

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 and penetration testing also provide awareness and training opportunities beyond the monitoring objectives; and
- **Scanning:** reviewing the internal and external environments for changing or emerging risk. The aim is to provide an early appreciation of emerging issues to allow sufficient time to act upon them. Although virtually essential at a strategic level, it should be adopted as a monitoring practice at all levels of the organisation.

### 7.9.2 Triggering Monitoring & Review Processes

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

- Significant structural or layout changes are made to the Building, or neighbouring premises;
- Significant changes to critical assets occur (e.g. new types of equipment purchased, changes in the confidential nature of information being used/stored, departure of staff with knowledge of access to potential vulnerabilities);
- Significant changes occur in the local security environment (e.g. increase in offences locally, or increased exposure/publicity of University/Faculty);
- The national security threat changes significantly (eg the National Terrorism Public Alert levels etc);
- Management responsibilities change significantly (e.g. appointment of a new Chancellor);
- New contractors/suppliers are appointed;
- Controversial research undertaken within UoN NeWspace Building, or within the University in general;
- Availability and utility of security related technology changes;
- There are significant changes in the nature of security risk within similar industries, markets, etc;
- Mergers/amalgamation/privatisation are occurring; and
- Significant new 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, organisation or individual;
- The incidence, nature, types and impacts of security risk;
- The changing acceptability or tolerance of risk by the individual, organisation, community, or by their stakeholders;
- The effectiveness of security risk controls; and
- The effectiveness of security awareness programs and other communications initiatives.

### 7.9.3 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;

## DRAFT

- 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.

# DRAFT

## 8.0 Recommendations

### 8.1 CPTED Measures

- Where practical, incorporate the following CPTED measures within the works areas;
- Provide clear definition and designation of space in a manner that encourages and predicts authorised movement and does not cause conflict between the intended purpose of the space and the desired behaviour;
- Facilitate clear sightlines and maximise pedestrian circulation areas by:
  - Minimising built structures and avoiding clutter, particularly along main thoroughfares and at main building entry/exit points, and
  - Maximising natural, passive and active surveillance opportunities from the inside and external of the structure.
- Provide lighting design which conforms to Australian and University Standards and provides well lit and uniform lighting throughout the Building and its surrounding areas that promote passive and active surveillance;
- Keep vegetation around the Building well maintained and to a low height, to reduce places for concealment of activities, places for potential offenders to hide, and to enhance the natural and active surveillance of the area;
- Provide vandal resistant fittings and graffiti resistant surfaces where practical, which promotes the prompt repair and cleaning of vandalism and graffiti; and
- Provide security signage to inform the public of restricted and dangerous areas, and to notify them that security measures are in place (eg CCTV used in the area).

### 8.2 Physical Security Measures

- Provide high security locking devices, well-constructed doors, door frames and door hardware where practical, to provide a level of resistance against forced entry into buildings; and
- Physical security devices and building construction methods to provide a high level of resilience to forced entry.

### 8.3 Electronic Security Measures

#### 8.3.1 EACS

- Provide electronic access control to nominated doors to electronically control access into/out of these areas, and to provide an audit function.

#### 8.3.2 IAS

- Provide reed switches to nominated doors to monitor their integrity (open/closed/door-open-too-long/forced door).
- Provide passive infra-red volumetric detectors to monitor the integrity of a nominated area.

#### 8.3.3 CCTV

- Provide a CCTV system to monitor nominated areas, to provide a deterrence against antisocial behaviour, and to provide evidence capturing abilities.

#### 8.3.4 Emergency Help Points and Duress

- Provide emergency help points, and fixed duress alarms to nominated locations to allow students and staff to call for assistance during emergency situations.

# DRAFT

## 8.4 Information Security Measures

- Communications rooms to be adequately secured by high security locking devices/EACS and monitored via magnetic reed switches;
- Head-end communications equipment to be securely stored within lockable communications racks;
- Sensitive information to be stored according to University 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;
- Adequate IT security measures to be provided to protect IT infrastructure and University information against attack; and
- Perform regular backups of data.

## 8.5 Operational Security Measures

- Formulation (or review if existing) of comprehensive Standard Operating Procedures for all staff/contractors who will have an operational role at the UoN NeW Space Building;
- Determination of adequate security monitoring capabilities and assignment of monitoring responsibilities, either locally (at security desk) or at the Security Services Office, or a combination of each;
- Assignment of effective response personnel and procedures associated with the safe response to security incidents;
- Implementation of a detailed security incident reporting system for the UoN NeW Space Building to allow accurate capturing and reporting of incidences. Recorded incidences should be used when monitoring and reviewing the risk profile at the University;
- Ongoing and systematic training and inductions of staff, contractors and visitors; and

## 8.6 Security Management Measures

- University of Newcastle to continuously monitor the risks and the effectiveness of security treatment measures through post event analysis and reporting, and liaison with NeW Space stakeholders and the Security Department. Periodic reviews of the security risks should be performed. Security risks should also be reviewed at the initial stage of any capital works program occurring at the site.



**D R A F T**

Appendix A

# Security Risk Matrix

**DRAFT**

Appendix A Security Risk Matrix

## UoN NeW Space Risk Register

Serial #	Risk Identification Process				Pre-Treatment Risk Level			Post Treatment Risk Level		
	Asset most likely at Risk (People, Property, Information, etc)	Identified Risk	Description of Risk (i.e. Example of Risk Eventuating)	Most Likely Source of Threat (Who poses the greatest Threat?)	Likelihood	Consequence	Risk Rating	Likelihood	Consequence	Risk Rating
1	Reputation	Facility Location & Exposure	Increased media or exposure due to prominent Building location, University reputation, conducting any controversial research	PM/IM Groups	Possible	Moderate	M	Possible	Minor	M
2	Information	Unauthorised Access - Pedestrian (Trespass)	Unauthorised pedestrian access to the Building areas resulting in possible theft, vandalism, sabotage to equipment, loss of IP, harm to staff, etc	Public	Possible	Minor	M	Unlikely	Minor	L
3	Property / Equipment	Unauthorised Access - Vehicle	Unauthorised vehicle access (e.g. tailgating, illegal parking, etc) during or after hours resulting in illegal access to the Building areas	Visitors	Possible	Insignificant	L	Unlikely	Insignificant	L
4	Property / Equipment	Forced Access - Pedestrian (Break and Enter)	Forced pedestrian access or entry to the Building areas resulting in possible theft, vandalism or sabotage to equipment, harm to staff, etc.	PM/IM Groups	Possible	Moderate	M	Unlikely	Moderate	M
5	Property / Equipment	Forced Access - Vehicle	Forced vehicle access (e.g. ram raid) during or after hours resulting in illegal access to the Building areas	PM/IM Groups	Unlikely	Moderate	M	Rare	Moderate	L
6	Property / Equipment	Mechanical failure of security equipment	Failure of equipment due to poor maintenance regimes	PM/IM Groups	Possible	Minor	M	Unlikely	Minor	L
7	People	Breakdown of access control measures for specific areas	Intrusion of non-authorised people into secure areas within the Building	PM/IM Groups	Possible	Minor	M	Unlikely	Minor	L
8	Reputation	Protest or Demonstration - Non-Violent	Non-violent protest or demonstration by Issue Motivated Groups resulting in illegal occupation of the the Building, unwanted media exposure, interruption to operations, etc	Students	Possible	Insignificant	L	Possible	Insignificant	L
9	People	Protest or Demonstration - Violent	Violent protest or demonstration by Issue Motivated Groups resulting in forced or unauthorised access to the Building, illegal occupation, unwanted media exposure, with major interruption or cessation of operations, possible injury or harm to staff, damage to buildings and property, etc	PM/IM Groups	Unlikely	Major	M	Unlikely	Moderate	M
10	Information	Compromise of university/faculty information	Inappropriate management and storage of security related information	PM/IM Groups	Possible	Minor	M	Unlikely	Minor	L
11	People	Unauthorised obtainment of access card	Use of compromised access card (lost / stolen card)	PM/IM Groups	Unlikely	Insignificant	L	Unlikely	Insignificant	L
12	Property / Equipment	Mechanical failure critical building services/equipment	Failure of building services to operate continuously	PM/IM Groups	Possible	Moderate	M	Unlikely	Moderate	M
13	Property / Equipment	Breakdown of security policies and procedures	Compromise of key system	PM/IM Groups	Unlikely	Insignificant	L	Unlikely	Insignificant	L
14	People	Insider assistance	Compromise of Security Staff/ general staff/ contractors	Compromised or influenced staff	Rare	Major	M	Rare	Major	M
15	People	Receipt of Suspect Substances - Mail (eg white powder, anthrax, C4, etc)	Receipt of mail or other packages containing suspect substances, explosives or incendiary devices resulting in disruption to operations, emergency evacuation, injury to staff, property or possible loss of life.	PM/IM Groups	Unlikely	Major	M	Unlikely	Moderate	M
16	People	Murder / Manslaughter	students/staff/contractors/general public	Public	Rare	Major	M	Rare	Major	M
17	People	Physical assault	students/staff/contractors/general public	Public	Possible	Minor	M	Possible	Minor	M
18	People	Verbal assault	students/staff/contractors/general public	Public	Possible	Insignificant	L	Possible	Insignificant	L
19	People	Sexual assault	students/staff/contractors/general public	Public	Possible	Minor	M	Possible	Minor	M
20	People	Indecent assault	students/staff/contractors/general public	Public	Possible	Minor	M	Possible	Minor	M
21	People	Offensive conduct	students/staff/contractors/general public	Public	Possible	Insignificant	L	Possible	Insignificant	L
22	People	Abduction and kidnapping	students/staff/contractors/general public	PM/IM Groups	Rare	Moderate	L	Rare	Moderate	L
23	People	Harassment, threatening behaviour and private nuisance	students/staff/contractors/general public	Public	Likely	Insignificant	M	Likely	Insignificant	M
24	People	Robbery	students/staff/contractors/general public	Opportunists	Possible	Minor	M	Possible	Minor	M
25	Property / Equipment	General Theft - organised crime	Theft of property, equipment or information resulting in financial loss to the Building/Faculty/University, cessation or interruption to services, loss of personal property, embarrassment or impact to reputation, etc	Criminal Groups	Unlikely	Minor	L	Unlikely	Minor	L
26	Property / Equipment	Targeted Theft	Theft of property, equipment or information resulting in financial loss to the Building/Faculty/University, cessation or interruption to services, loss of personal property, embarrassment or impact to reputation, etc	Opportunists	Almost Certain	Minor	H	Likely	Minor	M
27	Property / Equipment	Theft - Opportunist	Theft of equipment/assets from theatres/library/teaching spaces/student hub/offices etc	Opportunists	Almost Certain	Minor	H	Likely	Minor	M
28	People	Drug/Alcohol offences	Intoxicated persons posing a risk to themselves or others	Public	Almost Certain	Minor	H	Likely	Minor	M
29	People	Terrorist Type Activities	Targeted attack to cause high loss of life / chaos, Designed to achieve maximum casualties to people In the vicinity of target - Targeting high density population or meeting areas.	PM/IM Groups	Rare	Catastrophic	M	Rare	Catastrophic	M

## UoN NeW Space Risk Register

Serial #	Risk Identification Process				Pre-Treatment Risk Level			Post Treatment Risk Level		
	Asset most likely at Risk (People, Property, Information, etc)	Identified Risk	Description of Risk (i.e. Example of Risk Eventuating)	Most Likely Source of Threat (Who poses the greatest Threat?)	Likelihood	Consequence	Risk Rating	Likelihood	Consequence	Risk Rating
30	People	Active shooter	Sniper or roaming shooter aimed at maximum casualties in an open environment	PM/IM Groups	Rare	Catastrophic	M	Rare	Catastrophic	M
31	Information	Bomb threat warning	To cause delay and disruption to services and events. Potential use as intelligence gathering on response procedures, prior to genuine attack	PM/IM Groups	Rare	Moderate	L	Rare	Moderate	L
32	Property / Equipment	Vandalism / graffiti	General by criminals, opportunists, youths, gangs etc	Opportunists	Almost Certain	Insignificant	M	Likely	Insignificant	M
33	Property / Equipment	Vandalism / graffiti	Targeted by politically motivated groups, issue motivated groups, anarchists etc	PM/IM Groups	Possible	Insignificant	L	Unlikely	Insignificant	L
34	People	Arson	Intentional acts to set fire to the Building facilities to cause damage or destruction to property and equipment, information or people.	PM/IM Groups	Rare	Catastrophic	M	Rare	Major	M
35	Information	Espionage - Industrial	Conduct of intelligence gathering activities by Competitor (of any private enterprise research partners) or Issue Motivated Group (i.e. industrial espionage) with intention to obtain or steal information, gain competitive advantage, personnel details etc.	PM/IM Groups	Rare	Major	M	Rare	Major	M
36	Property / Equipment	Sabotage	Sabotage of property or equipment etc by a person or group with intent to cause damage resulting in cessation or interruption to Building/Faculty/University operations, loss or corruption of information etc	PM/IM Groups	Rare	Major	M	Rare	Major	M
37	Property / Equipment	Loss of Power or Building Services	Loss of power or critical services to the the Building due to breach of building security to gain access to critical plant areas containing power distribution equipment, mechanical and/or other services, etc resulting in damage or sabotage to building infrastructure and cessation of services, or damage to the power feeders that provide power to the overall plant, either externally to the site or at the main transformer building.	PM/IM Groups	Unlikely	Major	M	Unlikely	Major	M
38	Information	Physical attack against IT or Communications infrastructure	Attack against LAN/WAN networks, computer or server rooms, public power or communications infrastructure, etc resulting in loss or cessation of services to the the Building/faculty/University	PM/IM Groups	Unlikely	Major	M	Unlikely	Major	M
39	Information	Information / data resources	Targeted attack to cause loss / destruction / modification / fabrication / disclosure / interception / interruption / denial of service to the Building physical and electronic information/data	Criminal Groups	Unlikely	Major	M	Unlikely	Major	M
40	Information	Unauthorised or inadvertent disclosure of sensitive information	Unauthorised or inadvertent disclosure of sensitive information 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.	Staff (Internal Threat)	Possible	Minor	M	Possible	Minor	M
41	Information	Unauthorised Access to Security Head-End Equipment	Unauthorised access to security communications racks	Staff (Unintentional Threat)	Possible	Minor	M	Possible	Minor	M