

Station Hill. Reading. SH Reading Master LLP.

SECURITY
SECURITY STRATEGY REPORT

REVISION 02 – 19 SEPTEMBER 2019



STAGE 2

Audit sheet.

Rev.	Date	Description of change / purpose of issue	Prepared	Reviewed	Authorised
01	31/01/2019	Issue (Phase 1)	DC	RJ	RJ
02	19/09/2019	Issue (Phase 1, 2 and 3)	DC	RJ	RJ

This document has been prepared for SH Reading Master LLP only and solely for the purposes expressly defined herein. We owe no duty of care to any third parties in respect of its content. Therefore, unless expressly agreed by us in signed writing, we hereby exclude all liability to third parties, including liability for negligence, save only for liabilities that cannot be so excluded by operation of applicable law. The consequences of climate change and the effects of future changes in climatic conditions cannot be accurately predicted. This report has been based solely on the specific design assumptions and criteria stated herein.

Project number: 25-25046
Document reference: REP-2525046-XX-DC-20190809-Station Hill security strategy-Rev02

Contents.

Audit sheet.	2
Executive summary	4
What are we trying to protect?	4
What do we need to protect it from and where?	4
How do we propose to protect it?	4
1. Introduction	5
1.1 Overview	5
1.2 Approach	5
1.3 Report structure	5
1.4 BREEAM NC 2018 HEA 06	5
2. What are we trying to protect?	7
3. What do we need to protect it from and where?	8
3.1 Threat overview	8
3.2 Threat discussion	8
3.3 Risk identification and analysis	8
4. How do we propose to protect it?	10
4.1 Overview	10
4.2 Design constraints and assumptions	10
4.3 Operational requirements	10
Appendix A – Context analysis	13
Project overview	13
Project site description	13
Adjacencies analysis	14
Security stakeholders and user groups	15
Key references	15
Design constraints and assumptions	15
Context analysis key findings / conclusions	16
Appendix B – Identify and categorise assets	17
Overview	17
Assets identification	17
Asset analysis	17
Appendix C – Vulnerability identification	18

Overview	18
Vulnerability identification and analysis	18
Vulnerability relationships	21
Appendix D – Identify threats	22
Overview	22
Threat assessment	22
Information sources	22
Threat analysis – Design basis threats	22
Threat discussion	22
Appendix E - Identify and analyse risks	28
Overview	28
Risk evaluation	28
Appendix F - Develop security strategy	46
Operational Requirements	46
Operation Requirements (ORs) identification	46
Phase specific strategies	46
Security strategy graphic	48
Security strategy (zoning) drawings	48
Appendix H – Phase 2 (1 Station Hill Plaza, The Rest and surrounding podium level)	49
Security strategy graphic	49
Security strategy (zoning) drawings	49
Appendix I – Phase 3 (Plots A, B, C, D and the basement levels, including the parking)	50
Security strategy graphic	50
Security strategy (zoning) drawings	50

Executive summary

This report examines the security risks to the Station Hill development, a residential, commercial and retail development in Reading, and proposes a strategy for managing them. It follows a risk assessment methodology and presents the strategy in the form of Operational Requirements (ORs) as recommended by the Centre for Protection of National Infrastructure (CPNI) and the UK Police.

The intention is to provide a common, agreed, understanding of the ‘security needs’ and communicate the security strategy required as a basis for subsequent design development.

A site wide strategy has been produced and been applied to the individual plots within the development.

Three fundamental questions have been applied which will help determine the appropriate processes to implement:

- What are we trying to protect?
- What do you need to protect it from and where?
- How do we propose to protect it?

What are we trying to protect?

The assets identified for consideration as part of this review are detailed below. These are considered the component parts, or processes, of the development that have the potential to be targeted by a credible threat.

We categorise assets into four broad areas:

People - Residential tenants, residential visitors, residential facility management and security staff, commercial employees, commercial visitors, commercial facility management and security staff, retail employees, retail visitors, retail facility management and security staff, FM contractors, delivery staff, public.

Property - Corporate property, personal property, retail property, residential property, building infrastructure, building envelope, third party assets.

Processes and services - Residential movement (tenant), residential movement (visitors), commercial movement (employees), commercial movement (visitors), retail movement (employees), retail movement (visitors), FM essential services, daily operations (incl. deliveries).

Knowledge and intellectual property - Personal records, corporate information.

What do we need to protect it from and where?

In our opinion, based on current police and government advice as well as a review of recent events, there are 12 design basis threats to the development. These are listed below.

Threat no.	Design Basis Threat	Threat no.	Design Basis Threat
T01	Explosive threat	T09	Burglary
T02	Vehicle as a weapon (VAW)	T10	Theft of (or from) a motor vehicle
T03	Close quarter attacks – solo	T11	Criminal damage and arson
T04	Close quarter attacks - coordinated	T12	Violent crime including attacks against the person and robbery.
T06	Insider threat (including radicalisation)	T13	Trespass
T08	Theft	T15	Antisocial behaviour and public order

An indicative introduction to the correspondence between the threats and the vulnerabilities within the development can be seen in Figure 4.

How do we propose to protect it?

To mitigate these risks, proportionate mitigation measures and the ORs listed below have been generated.

Provide a zoned approach to the development

A zoned approach, aligned with the understood operational needs of each individual plot, will be applied to the development that supports security layering / defence in depth and aids further security systems design.

Provide surveillance to monitor activity

Surveillance will be provided to the public realm and all access points, circulations areas and identified locations of each plot, where threats may manifest.

Provide controls to pedestrian access and circulation

Pedestrian access and circulation will be controlled by the use of physical barriers, doors, and electronic & mechanical access control measures, to align with the zonal approach and support vertical and horizontal separation of user groups.

Provide controls to vehicular access and movement

All vehicle threats to the development have been considered and addressed within a separate Vehicle Threat Mitigation Strategy document (REP-2525046-02-DC-20190531-Station Hill HVM-Rev01).

Provide physical security measures (general)

Physical measures will be utilised at locations such as, but not limited to, points of vehicle control, points of access and egress through the building envelopes and identified locations to provide extra protection against unauthorised access or removal of assets.

Provide communication to support security operations

Audio visual intercoms to support access and egress and panic alarm facilities to support calls for assistance will be located throughout the development at identified locations.

Provide security lighting to support surveillance

Lighting will be applied to support natural and electronic surveillance throughout the development, as well as eliminating secluded spaces and provide a greater “secure feeling” to users.

Provide ability to detect intruders

Unauthorised access or attempted access to the development and certain vulnerabilities needs to be detected in order for a suitable response to be initiated. Measures will be applied on points of access to the development and identified areas of importance to support security layering / defence in depth.

Provide operational security management

Appropriate operational policies, procedures and facilities will be in place to support security operations and reinforce technical and physical security design interventions.

Provide technical infrastructure to support security requirements

Many of the security measures require physical and technical infrastructure to support them, be that spatial or network infrastructure. This will be within each plot to support independent running of each plot.

The detailed strategy to implement these requirements is shown in the main report and in appendices G, H and I.

1. Introduction

1.1 Overview

The Station Hill project is a residential, retail and commercial development located in Reading. The purpose of this security strategy report is to identify and analyse the security risks to the development, then produce a comprehensive, but proportionate set of operational requirements as a basis for subsequent design development.

This security strategy aims to address 3 fundamental questions:

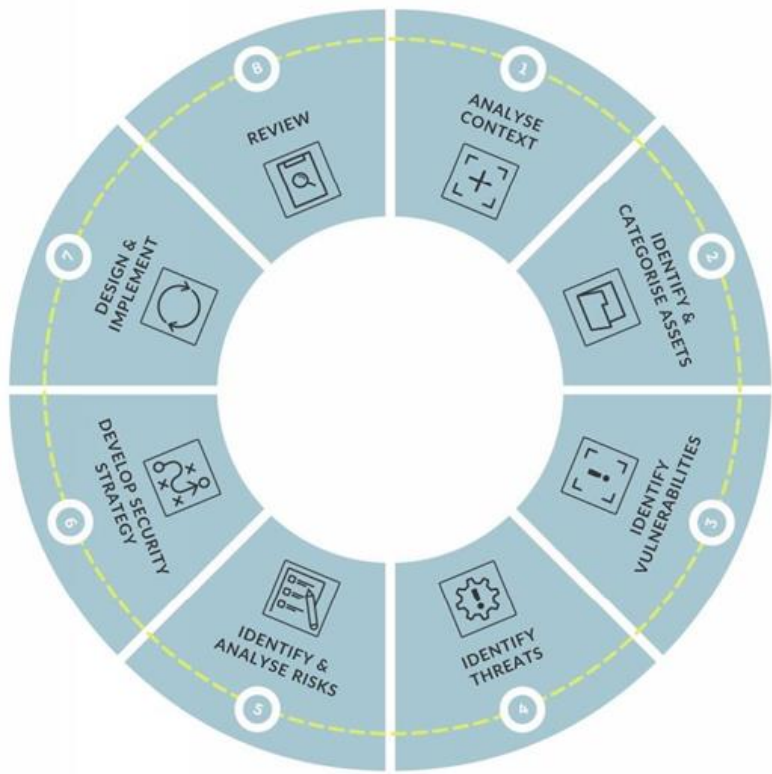
- What are we trying to protect?
- What do we need to protect it from and where?
- How do we propose to protect it?

1.2 Approach

A risk-based, threat-informed, systems approach to security engineering design. Our approach is completely aligned with the advice of CPNI, the national technical authority for protective security. Our approach to security design is the 8-stage cycle in Figure 1.

Key to our approach is the link between each successive iteration of detail as the Operational Requirement develops into a detailed design – we call this the “golden thread” and an essential part of our methodology is ensuring that this can be traced right through the design: from the initial threat right down to the final delivered component or construction detail. This ensures that value for money is not only delivered but can withstand robust interrogation at all stages in the project.

Figure 1. Hoare Lea security risk assessment methodology



Source: Hoare Lea

1.3 Report structure

Given the splitting of the development into three phases, phase 1 being the south side of the development and phases 2 and 3 to the north, this strategy report will take the form of a full site-wide risk assessment and three additional appendices, each individually addressing each phase.

1.4 BREEAM NC 2018 HEA 06

It is understood that the development will be pursuing BREEAM accreditation. A summary of Hoare Lea’s compliance with, and alignment to, HEA 06 can be seen in Table 1.

Table 1. HEA 06 alignment

HEA 06 requirement	SRA compliance and alignment
A Suitably Qualified Security Specialist (SQSS) conducts an evidence-based Security Needs Assessment (SNA) during or prior to Concept Design (RIBA Stage 2 or equivalent).	This report has been reviewed by David Croft, who meets the SQSS criteria and authorised by Richard Jones, who is registered SQSS with BRE. (http://www.redbooklive.com/pdfdocs/redbook-vol2part7.pdf#zoom=100)
The SNA to include: A visual audit of the site and surroundings, identifying environmental cues and features pertinent to the security of the proposed development.	Appendix A
The SNA to include: Formal consultation with relevant stakeholders, including the local Area Liaison Officer (ALO), Crime Prevention Design Advisor (CPDA) & Counter Terrorism Security Advisor (CTSA) (as applicable), to obtain a summary of crime and disorder issues in the immediate vicinity of the proposed development.	Appendix A
The SNA to: Identify risks specific to the proposed, likely or potential use of the building(s).	Appendix A-E
The SNA to: Identify any detrimental effects the development may have on the existing community.	Appendix A
The SQSS develops a set of recommendations or solutions during or prior to Concept Design (RIBA Stage 2 or equivalent). These recommendations or solutions aim to ensure that the design of buildings, public and private car parks and public or amenity space are planned, designed and specified to address the issues identified in the preceding SNA.	Appendix E and Section: 4.3.1
The recommendations or solutions proposed by the SQSS are implemented. Any deviation from those recommendations or solutions will need to be justified, documented and agreed in advance with a suitably qualified security specialist.	To be confirmed by BREEAM assessor at project completion

Stakeholder engagement

Key engagement activities that have been undertaken to date, with the relevant stakeholders:

Internal:

- LPC. (Various dates).
- CRTKL. (Various dates)
- Gensler. (Various dates).

External:

- Thames Valley Police Designing Out Crime Officer (DOCO). (07/12/2018 and 01/08/2019)
- Thames Valley Police Counter Terrorism Security Adviser (CTSA)¹. (Facilitated during the DOCO meetings)
- Reading Borough Council. (07/12/2018)

Minutes from these external meetings are available upon request. All stakeholder input has been incorporated into the analysis contained in this report.

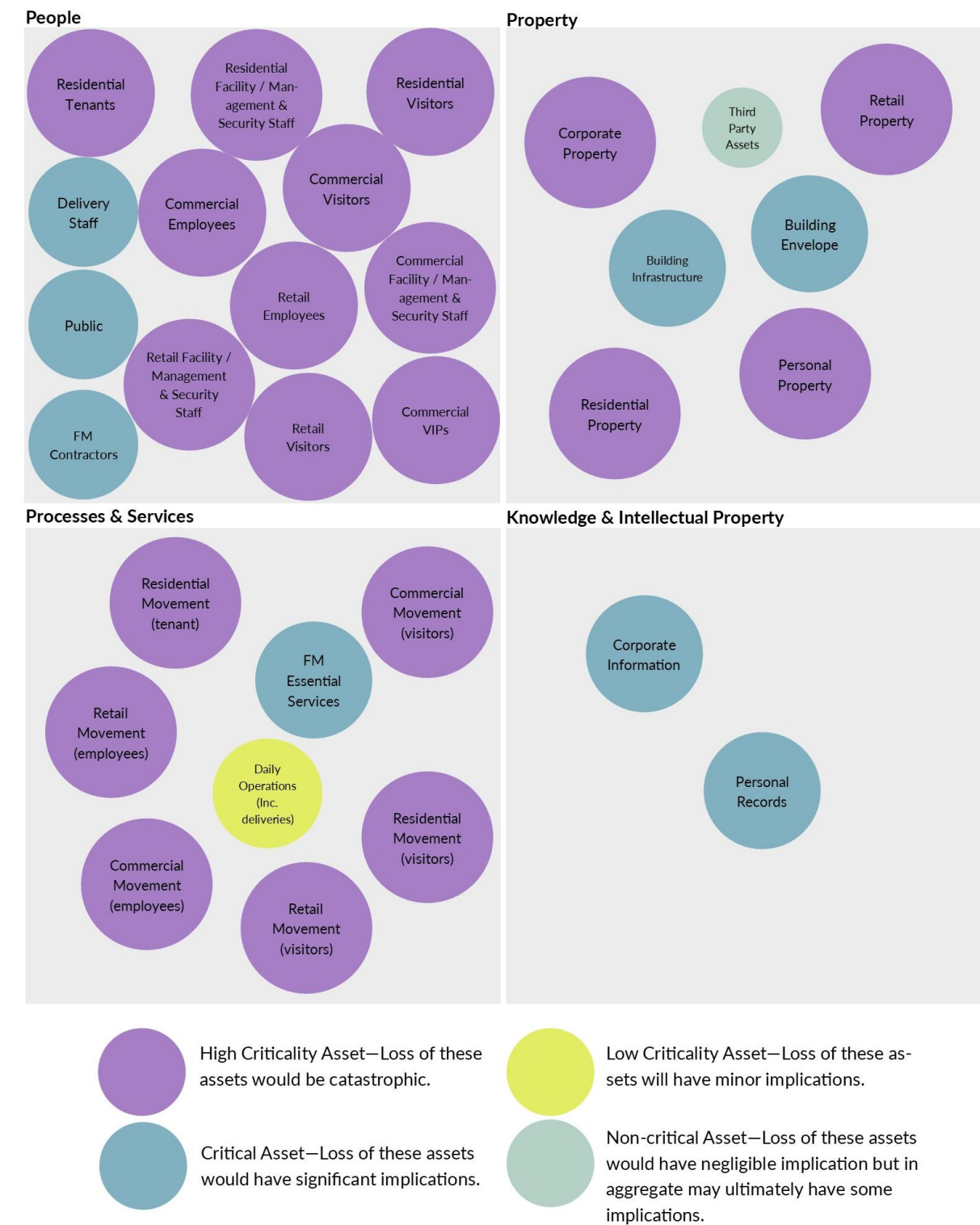
¹ Engaged by Thames Valley Police DOCO.

2. What are we trying to protect?

In order to develop an effective security strategy, what is being protected needs to be identified – the assets. We categorise assets into four broad areas: ‘people’, ‘property’, ‘processes and services, and ‘knowledge and intellectual property’. Furthermore, we identify those assets deemed most critical to the continued success of the development.

The asset identification and analysis can be seen in Appendix B. This is summarised in Figure 2.

Figure 2. Assets



Source: Hoare Lea

3. What do we need to protect it from and where?

3.1 Threat overview

A detailed threat assessment has been carried out. This has drawn on a number of sources of threat including open source police and government data and provides an assessment of the crime and terrorism threats posed to the project. It assesses the key threats, including those identified by security stakeholders, through an analysis of intent and capability from threat actors. It considers likely targets of the threats. The primary aims of the threat assessment are to identify the threats that are credible, thus forming the design basis threats (DBTs). The identified DBTs can be seen in Table 2.

Table 2. Design basis threats

Threat no.	Design Basis Threat	Threat no.	Design Basis Threat
T01	Explosive threat	T09	Burglary
T02	Vehicle as a weapon (VAW)	T10	Theft of (or from) a motor vehicle
T03	Close quarter attacks – solo	T11	Criminal damage and arson
T04	Close quarter attacks - coordinated	T12	Violent crime including attacks against the person and robbery.
T06	Insider threat (including radicalisation)	T13	Trespass
T08	Theft	T15	Antisocial behaviour and public order

3.2 Threat discussion

A number of DBTs warrant further discussion:

Explosive device (credible)

The threat from a person borne or placed device remains however, in the form of smaller devices being left in the public realm to target the crowd during events. It is unlikely that an explosive attack would be directed towards the structures, rather against a crowd in the public realm. Whilst a vehicle borne device is possible, given the proximity of a category A transport hub in the form of Reading station, and the crowds it generates on certain occasions, it is considered that will be the more attractive and accessible target.

Vehicle As a Weapon (credible)

The threats of a Vehicle As a Weapon are deemed credible. All vehicle threats to the development have been considered and addressed within a separate Vehicle Threat Mitigation Strategy document (REP-2525046-02-DC-20190531-Station Hill HVM-Rev01).

Violent crime (credible)

The crime statistics indicate that violent crime is a very significant factor in area and that due diligence should be done to mitigate it where possible.

Theft (credible)

According to the available crime statistics, the presence of theft and similar offences feature prominently in the area and therefore merit specific attention. The activation of the public realm with retail and occasional events, combined with the daily throughput of pedestrians to and from the station and hence the increase of personal effects within the accessible areas, will increase the likelihood of theft in all its forms.

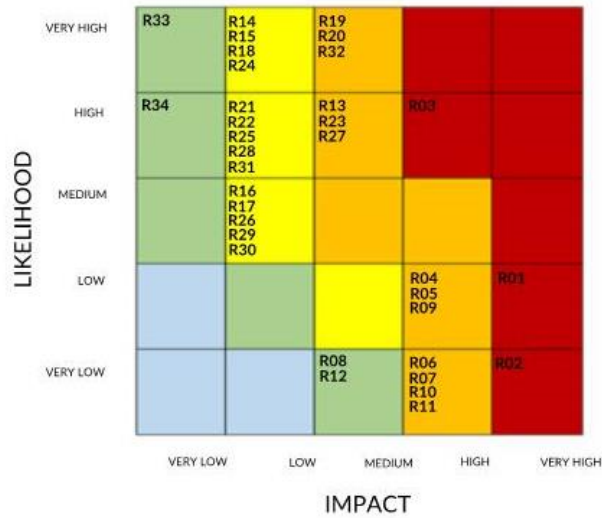
Anti-social behaviour (credible)

The crime statistics indicate that anti-social behaviour is a prominent challenge in the area. The activation of the public realm with retail and occasional events, combined with the daily thoroughfare of pedestrians to and from the station will increase the likelihood of anti-social behaviour and other threats that may manifest from an escalation of such behaviour. This will increase further on match days, due to the volume of exuberant match goers as they make their way to and from the station through the development.

3.3 Risk identification and analysis

A security risk exists where there is a likelihood that a threat can act within the development and produce an impact. The DBTs have been aligned to the vulnerabilities to determine the security risks that the development faces. These risks have been analysed to quantify the scale of the risks. In total 34 risks were identified and evaluated. This is summarised in the risk matrix in Figure 3.

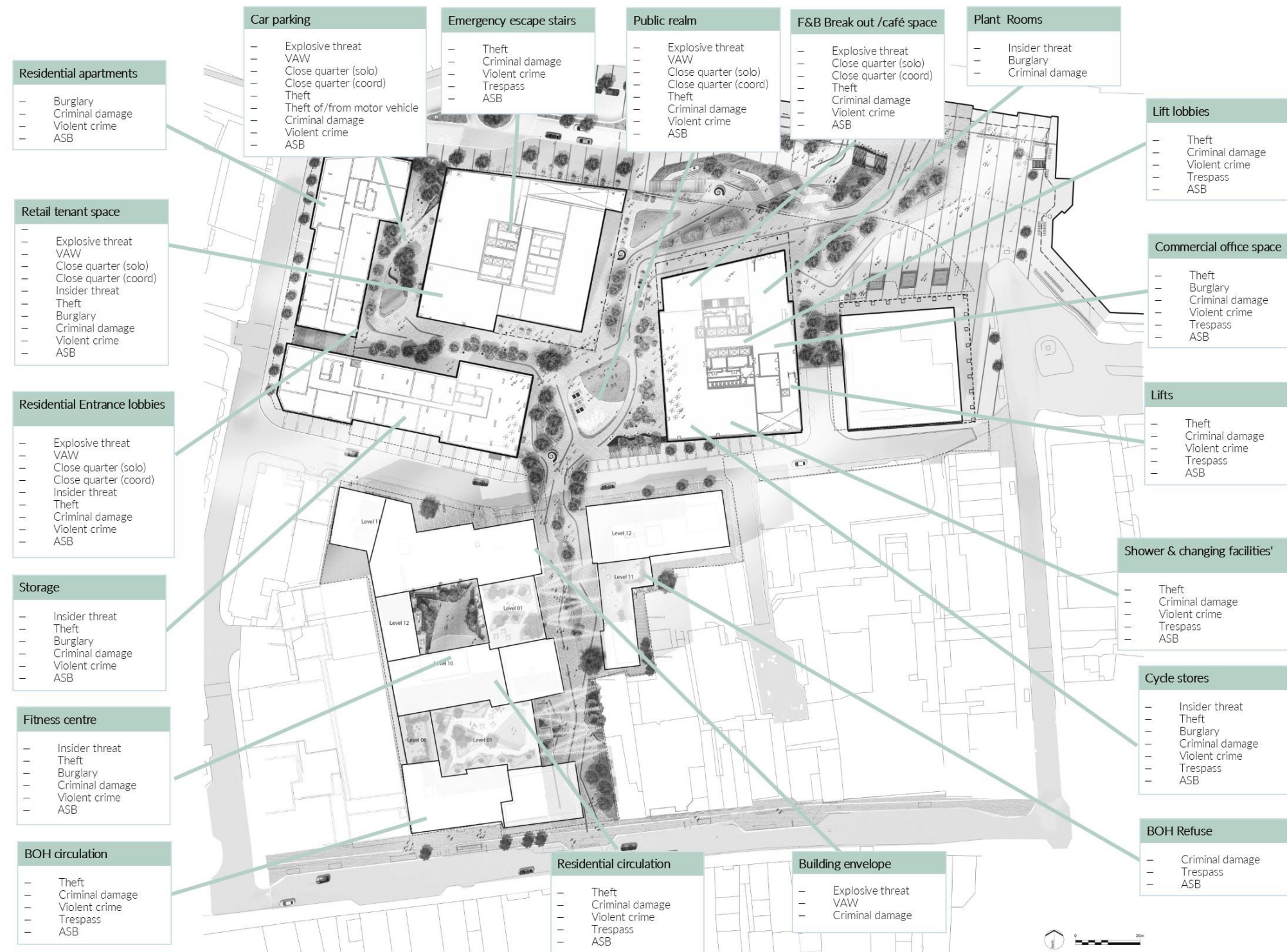
Figure 3. Risk matrix - gross risk



Risk treatments (how do we propose to protect it) are considered in the next section.

The risks are indicatively summarised development wide in the following Risk Summary Graphics (RSG) in Figure 4.

Figure 4. Risk summary graphic



Source: Hoare Lea

4. How do we propose to protect it?

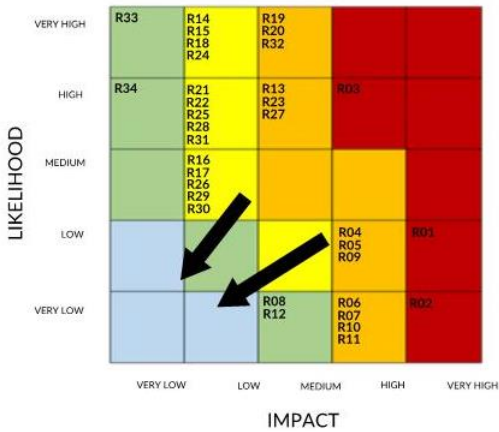
4.1 Overview

The security risk assessment has identified the security ‘needs’ of the development – what needs to be protected, and from what and where. The final part of this process is to determine appropriate risk treatments – how do we propose to protect it.

The intent of any risk treatment is to reduce the severity of those risks being treated in terms of likelihood and/or impact. We refer to these as gross risk (pre-treatment) and net risk² (post-treatment). This is also shown graphically in Figure 5. This net risk needs to be understood and accepted by the client – no risk treatment will eliminate risk completely.

It has been assessed as appropriate for the project that those risks graded medium, high and very high are treated and that any lower risks will benefit from the aggregated risk treatments applied to other risks (i.e. they will also benefit from the identified treatments). These treatments are addressed in later sections of this strategy document.

Figure 5. Risk matrix – Risk treatment intent



Source: Hoare Lea

We define these in terms of **Operational Requirements** (ORs). The ORs at this stage identify the effect, rather than the detail of each individual security measure (this is considered in a Detailed OR – addressed during the RIBA stage 3 design.) Combined, the ORs form the security strategy. Further detail on our approach to defining security strategies can be found at Appendix F.

4.2 Design constraints and assumptions

The following design constraints and assumptions have been identified:

- The location of the development places it in the proximity of a Cat A transport hub, namely Reading Station and this will have an influence on the northern elements of the developments Vehicle Threat Mitigation Strategy.
- The roof-top amenities in the commercial buildings will be controlled environments, including for the tenants. It is assumed that during the day they may be open, but during the evening they will need to be booked.
- The fitness facilities within the relevant plots are for tenants only.

² This is sometimes referred to as residual risk.

- The amazon lockers within the commercial buildings are there to accommodate tenant deliveries, but will be operationally managed, rather than tenant accessed.
- Each plot is required to have the ability to operate independently.
- A development wide, operational security management plan is yet to be devised.
- The commercial buildings will be occupied by multiple tenants.
- VIP lobbies in the basements of the commercial plots are only for limited users, not all tenant staff.

4.3 Operational requirements

Summary and indicative solutions

A summary of key recommendations and ORs can be seen below in Table 3. Within this table, indicative solutions and implications for the design team have been captured.

Table 3. Operational requirements summary and indicative solutions

Operational requirements	Implications and indicative solutions ³
Provide a zoned approach to the development – Ensure security zones are established that support strategic security layering / defence in depth.	– A security zoning strategy will support a layered approach and the application of technical security systems.
Provide surveillance to monitor activity – Provide surveillance measures in all lobbies, reception areas and the cafe. – Provide surveillance to monitor activity in the public realm and car parking. – Provide surveillance to monitor activity within the delivery service yards and BOH circulation. – Provide surveillance to monitor activity within the cycle storage. – Provide surveillance to monitor access to all plant rooms. – Provide surveillance to monitor activity within the post, all entrance lobbies, receptions, co-working space, café and meeting rooms. – Provide surveillance to monitor access to all office spaces. – Provide surveillance to monitor access to storage rooms, including, but not limited to the cycle store. – Provide surveillance to monitor access to the fitness centre, parcel delivery, office space gym and apartments. – Provide surveillance to all lift lobbies, lifts, goods lifts, VIP lifts lobbies, circulation and communal / shared amenities. – Provide surveillance to the public realm and throughout the development.	– Surveillance will be a mixture of natural and electronic surveillance (VSS/ CCTV) to be installed. – Natural surveillance throughout the development to be encouraged including views of approaches to the entrances. Any landscaping plan should consider future maintenance requirements to maintain sight lines. – Electronic surveillance of access points (internal and external) to enable identification of those entering.

³ All security measures are to have documented, detailed operational requirements developed during later design stages (formerly Level 2 Operational Requirements).

Operational requirements	Implications and indicative solutions ³
Provide controls to vehicular access and movement - Provide physical barriers and control of access measures to prevent unauthorised vehicle access to the public realm, car parks and service yard.	- Refer to Vehicle Threat Mitigation Strategy report REP-2525046-02-DC-20190531-Station Hill HVM-Rev01.
Provide controls to pedestrian access and circulation - Provide control of access between security zones in to control access and to deter or delay access. - Provide a minimum of two lines of control to gain access to all cores and circulation. - Provide control of access to all lift lobbies, lifts, circulation areas, VIP lift lobbies and amenities. - Provide vertical and horizontal compartmentalisation of floors. - Provide dynamic lock-down capability (including cores). - Provide control of access to the BOH circulation. - Provide control of access to plant rooms. - Provide control of access to the post, co-working space and meeting rooms. - Provide control of access to the office space (containment only). - Provide control of access to storage rooms. - Provide control of access to the gym, parcel delivery space, apartments.	- Universal tokens to be used by staff and guests, with a structured access group strategy. - Mechanical keys for plant, storage areas and other areas of similar activity. - External door-sets or gates to LPS 1175 SR2 or engineered equivalent. - Glazed curtain walling (if present) to BS EN 356-2000 (P1A) or engineered equivalent. - Apertures through building to be to LPS 1175 SR2. - Windows to be of commensurate security rating to surrounding doors and walls (LPS 1270 SR122). - Command and control facilities to support operational management (see operational management and technical infrastructure ORs). - EACS on doors requiring dynamic lockdown functionality - Pedestrian turnstiles in commercial buildings.
Provide physical security measures (general) - Provide physical barriers to all points of ingress and egress into the building through the building envelope. - Provide physical measures to reduce impact of any blast (e.g. stand-off, glazing enhancements) as appropriate to determined charge size. - Provide a physical barrier to the car parking. - Provide physical barrier to the delivery service yards. - Secure key cabinets and management protocols will be required. - Provide physical barriers to spaces containing high value items (eg. Cycle storage etc).	- Minimise depths of reveals and maintain natural surveillance / sight lines. - Glazed curtain walling (if present) to BS EN 356-2000 (P1A) or engineered equivalent. - Apertures through building to be to LPS 1175 SR2. - Ensure bike racks enable 3 points of locking.
Provide communication to support security operations - Provide ability for staff to raise alarm.	- Forms of communication connected to a security control room located at, but not limited to, main entrances, delivery bays, VIP lift lobbies, cycle storage entrances.

Operational requirements	Implications and indicative solutions ³
- Provide ability for audio and visual communication from key operational access-controlled points, such as, but not limited to the delivery service yards, car park entrances, cycle storage entrances and main entrances.	- Provide panic alarms (PAB) at the reception desk, Concierge desk, cashiers office, gym, pool.
Provide security lighting to support surveillance - Provide lighting throughout the development to support natural and electronic surveillance.	- Areas monitored by active surveillance (VSS) to have lighting in accordance with BS 5489, noting low level up-lighting can hinder identification through VSS. - Uniform lighting to the building envelope to comply with BS 5489.
Provide ability to detect intruders - Provide ability to detect unauthorised movement within or between security zones. - Provide ability to detect intrusion to restricted areas.	- Restricted areas likely to include plant rooms / areas, server rooms, security control room, etc., but to be defined in zoning strategy. - Command and control facilities to facilitate operational management (see operational management and technical infrastructure ORs).
Provide operational security management - Ensure security processes and procedures including security management plan, incident management and visitor, guest and contractor access approval.	- The development requires bespoke security management policies and procedures to deal with daily change of access permissions. Deliveries, security incidents, and to take appropriate responses. - Operational strategy to be defined at a later design stage.
Provide technical infrastructure to support security requirements - Provide command and control facilities to coordinate response and operational management. - Provide associated infrastructure to support electronic security systems.	- Location required for management PC to control user groups and issue access tokens on arrival for visitors, guests and contractors. - Command and control facilities with sufficient space, technical capability and manning to effectively handle the day to day operations and incidents that occur across the site including the ability to remotely control any active physical security measures. - Rack space required in server rooms – indicative space requirements: 1 rack requirement approximately 1m x 3m space. - Ability of security systems to be monitored remotely out of hours by a third party.

4.3.1 Security zoning strategy

The establishment of security zones is one of the key operational requirements that is identified in, and a key tenet of, any built asset development. This sets the baseline for security layering and the development of asset specific security measures during the next design stage.

Once layouts are frozen, this security zoning can also then be applied to these. The zonal strategy devised for the development can be seen below.

PUBLIC Accessible to everyone at all times with no ability to impose control measures	
SEMI PUBLIC Space that is easily accessible to the general public. Typically restricted outside of normal hours.	
SEMI-PRIVATE RESIDENTIAL Predominantly for the use of a limited, authorised population within residential spaces. Usually employs an electronic or procedural access control measure. Guests and visitors usually escorted.	
SEMI-PRIVATE COMMERCIAL Predominantly for the use of a limited, authorised population within commercial spaces. Usually employs an electronic or procedural access control measure. Guests and visitors usually escorted.	
SEMI-PRIVATE BOH Predominantly for the use of a limited, authorised population within BOH spaces. Usually employs an electronic or procedural access control measure. Guests and visitors usually escorted.	
SEMI-PRIVATE CO-WORKING Predominantly for the use of a limited, authorised population within commercial co-working spaces. Usually employs an electronic or procedural access control measure. Guests and visitors usually escorted.	
PRIVATE COMMERCIAL Private areas with limited access to authorised individuals (commercial employees). Guests usually escorted.	
PRIVATE RESIDENTIAL Private areas with limited access to authorised individuals (residential tenants). Guests usually escorted.	
PRIVATE LANDLORD BOH Private areas with limited access to authorised individuals (FM staff/BOH). Guests usually escorted.	
RESTRICTED Contain critical or sensitive assets and/or reserved for a very exclusive user group (i.e. security staff). Contractors may be allowed but would always be escorted.	

The security zoning strategy and subsequent application to the project general arrangement drawings have been captured and can be found in the phase specific appendices, G, H and I.

Appendix A – Context analysis

Project overview

The proposal is for the development of a new, high class multi-purpose destination and has been split into 3 phases for delivery.

Phase 1 consists of two residential plots, E & F, with limited retail elements and a public realm in the south of the development, between Garrard Street and Friar Street.

Phase 2 consists of 1 Station Hill Plaza (circa 25,000 sqm of offices), with retail elements, Station Hill Plaza, The Rest and the immediately surrounding parking levels on the north side of the development, between Station Hill / Reading Station and Garrard Street.

Phase 3 consists of residential plots (A, B & D) with a retail element, a commercial plot (C) with a retail element and the podium levels and parking on the north side of the development, between Station Hill / Reading Station and Garrard Street.

The relationship and split between Phases 1, 2 and 3 can be seen in Figure 6 with a proposed elevation in Figure 7.

Figure 6. Phase 1, 2 and 3



Source: Hoare Lea

Figure 7. Proposed elevation



Source: Lincoln MGT

Project site description

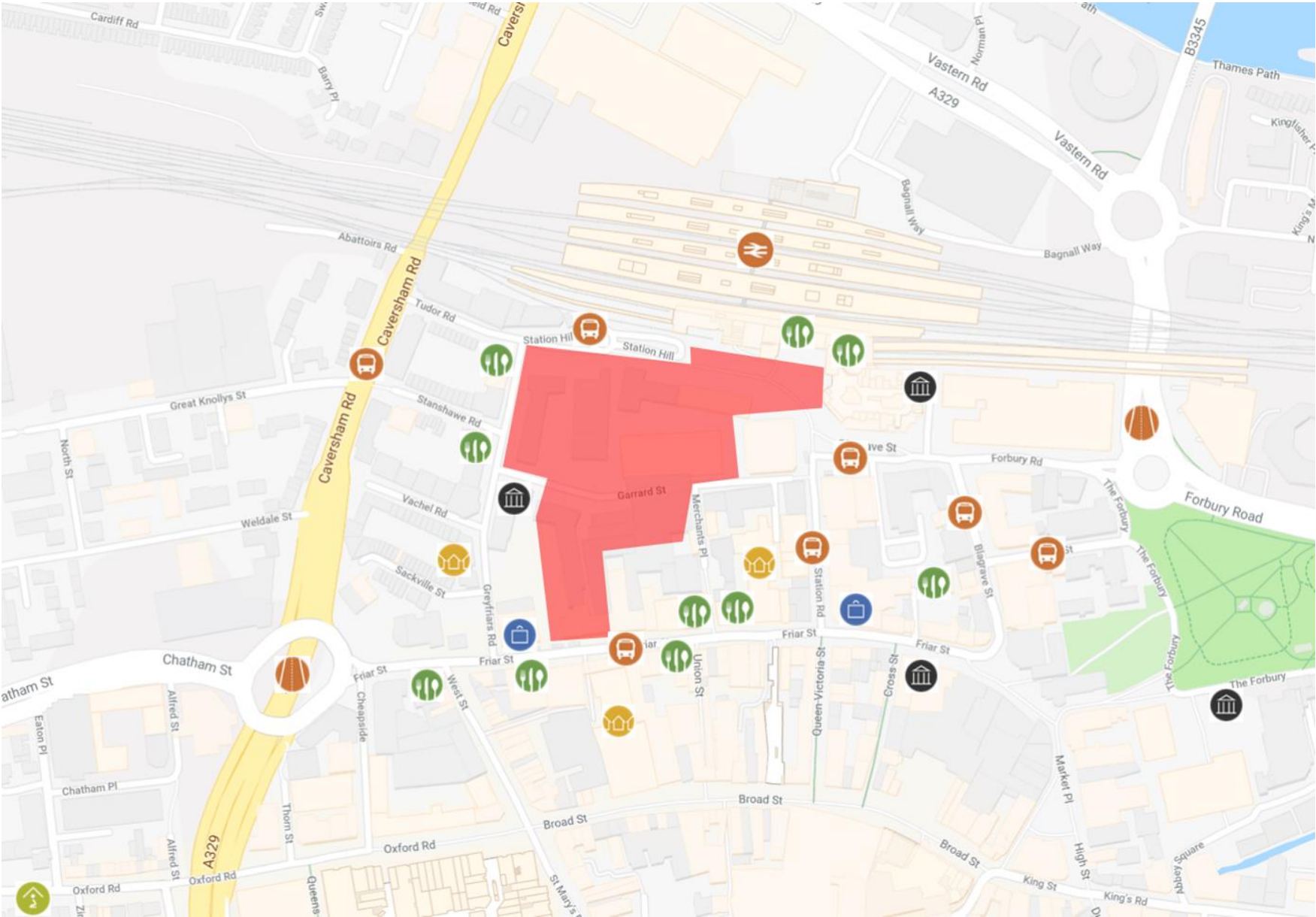
The site is strategically located in Reading, immediately next to Reading station and between the station and the town centre, see Figure 6. Surrounded by Greyfriars Road, Friar Street and Station Hill it has easy access to a variety of public transport networks and will be a thoroughfare for pedestrians travelling between the station and town centre.

Adjacencies analysis

An analysis of the surrounding area was undertaken to identify any possible influence it may have, Figure 8. A site visit was also carried out, in line with BREEAM requirements. The development is not incongruous to the surrounding area and is therefore not likely to represent a detrimental impact on the area.

Figure 8. Adjacencies

	The British Transport Police are based at Reading train station. The probation service offices and county court are in close proximity of the site.
	There are numerous food and beverage establishments on all sides of the development, meaning a high footfall in the area throughout the day and into the late evening. Friar Street, particularly due to its proximity of the south end of the development, hosts many clubs and bars which will have a significant impact on the levels of activity throughout the evenings.
	Reading train station is situated directly to the north of the site of the development. Given its proximity, this will lead to high volumes of foot traffic on that side of and through the development. The station also provides a primary transport capability for supporters attending football events at the stadium in the south of Reading (off the map), meaning significantly increased footfall on event days is highly likely in the development due to its location on the most direct pedestrian route.
	The area has a high number of bus routes servicing the surrounding area. The area is also serviced by night bus routes enabling easy access to large proportions of people 24/7.
	The site is flanked, at a distance, by Caversham Road to the West, Forbury Road to the east and on its perimeter, Friar Street to the south. Whilst not directly at the site's border, it will entail high volumes of vehicle traffic throughout the day and night.
	In the local area there is a significant amount of residential, which will add to the footfall throughout the development.
	The site is located within very close proximity of Reading town centre. This has a large impact on threats in the area, particularly those that are motivated from terrorism as both primary and secondary threats could impact the development. The town centre may also be a destination for large crowds visiting the town for events such as those held at the football stadium (located to the south of Reading)



Security stakeholders and user groups

Stakeholders

Key internal and external stakeholders of the project are outlined in Table 4.

Table 4. Key stakeholders

Internal	Comment
LPC	Development Manager
CRTKL	Architect and Lead Designer (Residential plots and car park below the office plots)
Gensler	Architect and Lead Designer (Commercial plots)
Hoare Lea LLP	Building services and Security consultant
DP9	Planning consultant
External	Comment
Reading Borough Council	Local Authority
Thames Valley Police Counter Terrorism Security Advisor	To be engaged by Thames Valley Police DOCO
Thames Valley Police Designing Out Crime Officer	Anne Chalmers

Stakeholder engagement

Key engagement activities that have been undertaken to date, with the relevant stakeholders:

Internal:

- LPC. (Various dates).
- CRTKL. (Various dates)
- Gensler. (Various dates).

External:

- Thames Valley Police Designing Out Crime Officer (DOCO). (07/12/2018 and 01/08/2019)
- Thames Valley Police Counter Terrorism Security Adviser (CTSA)⁴. (Facilitated during the DOCO meetings)
- Reading Borough Council. (07/12/2018)

Minutes from these external meetings are available upon request. All stakeholder input has been incorporated into the analysis contained in this report.

User groups

The primary user groups of the development are outlined in Table 5. These are identified to assist in the assessment of security risks later in this document, primarily around the understanding of their movement around the development.

Table 5. User groups

Serial	User group
01	Residential tenants
02	Residential visitors
03	Residential facility management and security staff
04	Commercial employees
05	Commercial visitors
06	Commercial VIPs
07	Commercial facility management and security staff
08	Retail employees
09	Retail visitors
10	Retail facility management and security staff
11	Delivery Staff
12	FM Contractors for the development
13	Public

Key references

The following key references documents have been used in the creation of this document:

- Building Regulations 2010, Approved Document Q: security, dwellings.
- National Planning Policy Framework 2018.
- Secured by Design guidance.
- BCO – Guide to specification 2019.

Design constraints and assumptions

The following design constraints and assumptions have been identified:

- The location of the development places it in the proximity of a Cat A transport hub, namely Reading Station and this will have an influence on the northern elements of the developments Vehicle Threat Mitigation Strategy.
- The roof-top amenities in the commercial buildings will be controlled environments, including for the tenants. It is assumed that during the day they may be open, but during the evening they will need to be booked.
- The fitness facilities within the relevant plots are for tenants only.
- The amazon lockers within the commercial buildings are there to accommodate tenant deliveries, but will be operationally managed, rather than tenant accessed.
- Each plot is required to have the ability to operate independently.
- A development wide, operational security management plan is yet to be devised.
- The commercial buildings will be occupied by multiple tenants.
- VIP lobbies in the basements of the commercial plots are only for limited users, not all tenant staff.

⁴ Engaged by Thames Valley Police DOCO.

Context analysis key findings / conclusions

- The project represents a significant development within the area.
- The development is not incongruous to the surrounding area and is therefore not likely to represent a detrimental impact on the area.
- The development will have a diverse range of users, some of which have distinct needs.
- The location of the development places it in the proximity of a Cat A transport hub, namely Reading station and on a main pedestrian route to the town centre and local football club, which will have an influence of pedestrian activity within its public realm and accessible facilities.

Appendix B – Identify and categorise assets

Overview

We define an asset as a component part of the site/development that stakeholders or users wish to protect. Assets can be both tangible (e.g. physical objects) and intangible (e.g. ideas).

Our analysis initially looks at the project context and the development intent and from this aims to identify those assets deemed most critical to the continued success of the development. We categorise assets into four broad areas:

- People
- Property
- Processes and services
- Knowledge and intellectual property

Assets identification

Our analysis has identified a number of assets in Table 6. These are considered the component parts, or processes, of the development that have the potential to be targeted by a credible threat. The understanding of these assets has been utilised in the analysis of vulnerabilities.

Within these identified assets it is also recognised that there are additional ‘minor’ assets such as personal possessions carried on the person that will also require protection. However, these are considered as standard assets that are present in all developments and will be secured through either the treatment afforded to the more critical ones, or the risk transferred to the individual as much as is practicable.

Asset analysis

The assets have been further analysed to identify their criticality. A qualitative approach is taken to this with the assets being classified as:

- High criticality asset
- Critical asset
- Low criticality asset
- Non-critical asset

Further descriptions of these definitions are included in Table 6.

Table 6. Assets to be protected

People	Property	Processes & services	Knowledge & intellectual property
Residential tenants	Corporate property	Residential movement (tenant)	Personal records
Residential visitors	Personal property	Residential movement (visitors)	Corporate information
Residential facility management and security staff	Retail property	Commercial movement (employees)	
Commercial employees	Residential property	Commercial movement (visitors)	
Commercial VIP's	Building infrastructure	Retail movement (employees)	
Commercial visitors	Building envelope	Retail movement (visitors)	
Commercial facility management and security staff	Third party assets	FM essential services	
Retail employees		Daily operations (incl. deliveries)	
Retail visitors			
Retail facility management and security staff			
FM contractors			
Delivery staff			
Public			

	High criticality asset - loss of these assets would be catastrophic to the development/system.
	Critical asset - loss of these assets would have significant implications on the operation of the development.
	Low criticality asset - loss of these assets will have minor implications on the operations of the system/development.
	Non-critical asset - loss of these assets would have negligible implications but in aggregate may ultimately have some implications on the system/development.

Appendix C – Vulnerability identification

Overview

For the purpose of a security risk assessment in the built environment, we define vulnerabilities as those parts of the built environment (spaces) where an asset may be targeted by a threat actor and a potential for impact exists.

Certain assets, e.g. staff must be considered as transient through the building and therefore areas of the building become vulnerabilities as they pass through them.

Vulnerability identification and analysis

A vulnerability assessment of the development has been completed and is detailed below in Table 7.

Table 7. Vulnerability identification

Vulnerability number	Vulnerability	Assets within space
Site wide		
V1	Public Realm	Residential tenants, Residential visitors Residential facility management and security staff, Commercial employees, Commercial visitors, Commercial facility, management and security staff, Retail employees, Retail visitors, Retail facility, management and security staff, FM contractors Delivery staff Public, Personal property, Third party assets, Daily operations (including deliveries).
V2	Car parking	Residential tenants Residential visitors Residential facility management and security staff Personal property Residential movement (tenant) Residential movement (visitors) Commercial employees, Commercial visitors, Commercial facility, management and security staff, Retail employees, Retail visitors, Retail facility, management and security staff, FM contractors Delivery staff Public, Personal property, Third party assets, Daily operations (including deliveries)

Residential		
V3	Residential building envelope	Building infrastructure
V4	Delivery service yard	Residential facility management and security staff Delivery staff Corporate property Personal property Third party assets Daily operations
V5	Entrance lobbies	Residential tenants, Residential visitors Residential facility management and security staff, Personal property FM contractors Delivery staff Third party assets Residential movement (tenant) Residential movement (visitors) FM essential services Daily operations (deliveries)
V6	Lifts	Residential tenants, Residential visitors Residential facility management and security staff, Personal property FM contractors Third party assets Residential movement (tenant) Residential movement (visitors) FM essential services
V7	Lift lobbies	Residential tenants, Residential visitors Residential facility management and security staff, Personal property FM contractors Third party assets Residential movement (tenant) Residential movement (visitors) FM essential services
V8	Emergency escape stairs ⁵	Residential facility management and security staff
V9	Communal/shared amenities	Residential tenants Residential visitors Residential facility management and security staff FM contractors Residential property Personal property Residential movement (tenant) Residential movement (visitors) FM essential services
V10	Cycle store	Residential tenants Residential visitors Personal property

⁵ During normal operation. In the event of an emergency, it will be assumed that these doors will be opened and access provided to all.

		Residential movement (tenant) Residential movement (visitors) Residential facility management and security staff
V11	Residential refuse	Residential tenants Residential visitors Residential facility management and security staff Personal property Residential movement (tenant) Residential movement (visitors)
V12	Plant rooms	Residential facility management and security staff Residential property Building infrastructure
V13	Residential circulation	Residential tenants Residential visitors Residential facility management and security staff FM contractors Personal property Third party assets Residential movement (tenant) Residential movement (visitors) FM essential services
V14	Apartments	Residential tenants Residential visitors Personal property Residential property Building infrastructure Personal records
V15	Gym	Residential tenants Residential facility management and security staff FM contractors Residential property Personal property Delivery staff Public
V16	Post	Residential tenants Personal property Residential facility management and security staff FM contractors Residential movement (tenant)
V17	Reception	Residential tenants Residential visitors Residential facility management and security staff FM contractors Personal property Residential movement (tenant) Residential movement (visitors)
V18	Storage	Residential tenants Personal property Residential facility management and security staff
V19	Residents terrace	Residential tenants Personal property Residential visitors

		Residential facility management and security staff Personal property
V20	BOH circulation	Residential facility management and security staff FM contractors Delivery staff
Commercial		
V21	Commercial building envelope	Building infrastructure
V22	Entrance lobbies	Commercial employees Commercial visitors Commercial facility management and security staff FM contractors Delivery staff Personal property Third party assets Commercial movement (employees) Commercial movement (visitors) FM essential services Daily operations
V23	Reception	Commercial employees Commercial visitors Commercial facility management and security staff FM contractors Delivery staff Personal property Third party assets Commercial movement (employees) Commercial movement (visitors) FM essential services Daily operations Personal records Corporate records
V24	Tenant Circulation	Commercial employees Commercial visitors Commercial facility management and security staff FM contractors Corporate property Personal property Third party assets Commercial movement (employees) Commercial movement (visitors) FM essential services
V25	Changing and shower facilities	Commercial employees Commercial facility management and security staff Personal property Commercial movement (employees)
V26	Cycle storage	Commercial employees Commercial facility management and security staff Personal property
V26	Fitness centre	Commercial employees Commercial facility management and security staff FM contractors Corporate property

		Third party assets
V28	VIP Lift lobbies	Commercial VIP's Commercial facility management and security staff Personal property Commercial movement (employees)
V29	Refuse	Commercial facility management and security staff FM contractors Corporate property
V30	Plant rooms	Commercial facility management and security staff Corporate property Building infrastructure
V31	BOH circulation	Commercial facility management and security staff FM contractors Third party assets Personal property FM essential services
V32	VIP lifts	Commercial VIP's Commercial facility management and security staff Personal property Commercial movement (employees)
V33	Public lifts	Commercial employees Commercial visitors Commercial facility management and security staff FM contractors Public Personal property Building infrastructure Third party assets Commercial movement (employees) Commercial movement (visitors)
V34	Tenant lifts	Commercial employees Commercial visitors Commercial facility management and security staff FM contractors Personal property Building infrastructure Third party assets Commercial movement (employees) Commercial movement (visitors)
V35	Emergency escape stair core	Commercial facility management and security staff
V36	Commercial F&B/cafe	Commercial employees Commercial VIP's Commercial visitors Commercial facility management and security staff FM contractors Public Corporate property Personal property Third party assets
V37	Meeting rooms	Commercial employees

		Commercial VIP's Commercial visitors Commercial facility management and security staff Corporate property Personal property Third party assets Commercial movement (employees) Corporate records
V38	Storage rooms	Commercial facility management and security staff Corporate property
V39	Tenant lift lobby	Commercial employees Commercial visitors Commercial facility management and security staff FM contractors Personal property Third party assets Commercial movement (employees) Commercial movement (visitors)
V40	Toilets	Commercial employees Commercial VIP's Commercial visitors Commercial facility management and security staff FM contractors Corporate property Personal property
V41	Co-working space	Commercial facility management and security staff FM contractors Commercial visitors Corporate property Personal property
V42	Goods lift	Commercial facility management and security staff FM contractors Corporate property FM essential services
V43	Fire fighting lobbies	Commercial facility management and security staff FM contractors Third party assets
V44	Office space ⁶	Commercial employees Commercial VIP's Commercial visitors Commercial facility management and security staff Corporate property Personal property Commercial movement (employees) Commercial movement (visitors)
V45	Terraces	Commercial employees Commercial VIP's Commercial visitors Commercial facility management and security staff Personal property

⁶ Containment only as fit out is tenants responsibility.

V46	Parcel delivery space	Commercial facility management and security staff Delivery staff Personal property Corporate property
V47	Delivery service yard	Commercial facility management and security staff Delivery staff Corporate property
Retail		
V48	Retail building envelope	Building infrastructure
V49	Tenant space	Retail employees Retail visitors Retail facility management and security staff Retail property Personal property Third party assets Retail movement (employees) Retail movement (visitors) FM essential services
V50	BOH circulation	Retail facility management and security staff FM contractors FM essential services
V51	Plant rooms	Retail facility management and security staff Corporate property Building infrastructure
V52	Refuse	Retail facility management and security staff FM contractors Retail property

Source: Hoare Lea

Furthermore, the physical relationship between the vulnerabilities has been analysed and captured in phase specific network diagrams in appendices G, H and I.

Vulnerability relationships

The development has been further analysed to understand where the identified assets may become vulnerable to potential threats – the vulnerabilities.

This is summarised in Figures 9 and 10, which also captures the physical relationship between the vulnerabilities.

Figure 9. Residential plots vulnerability relationships

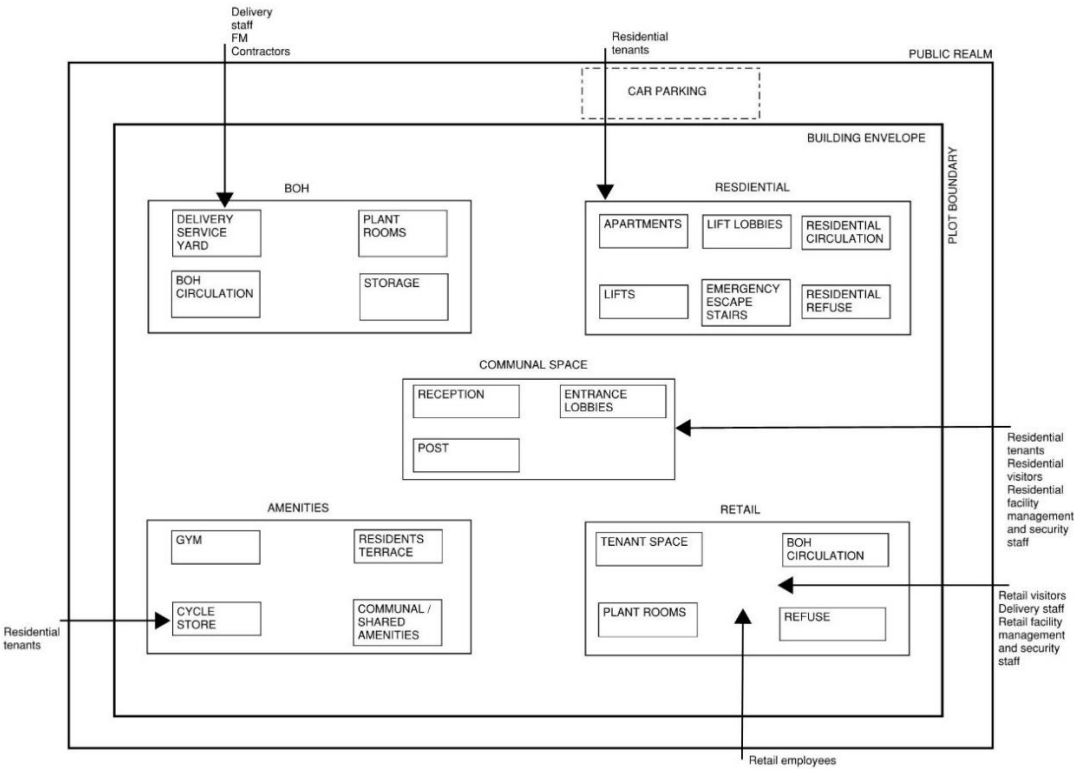
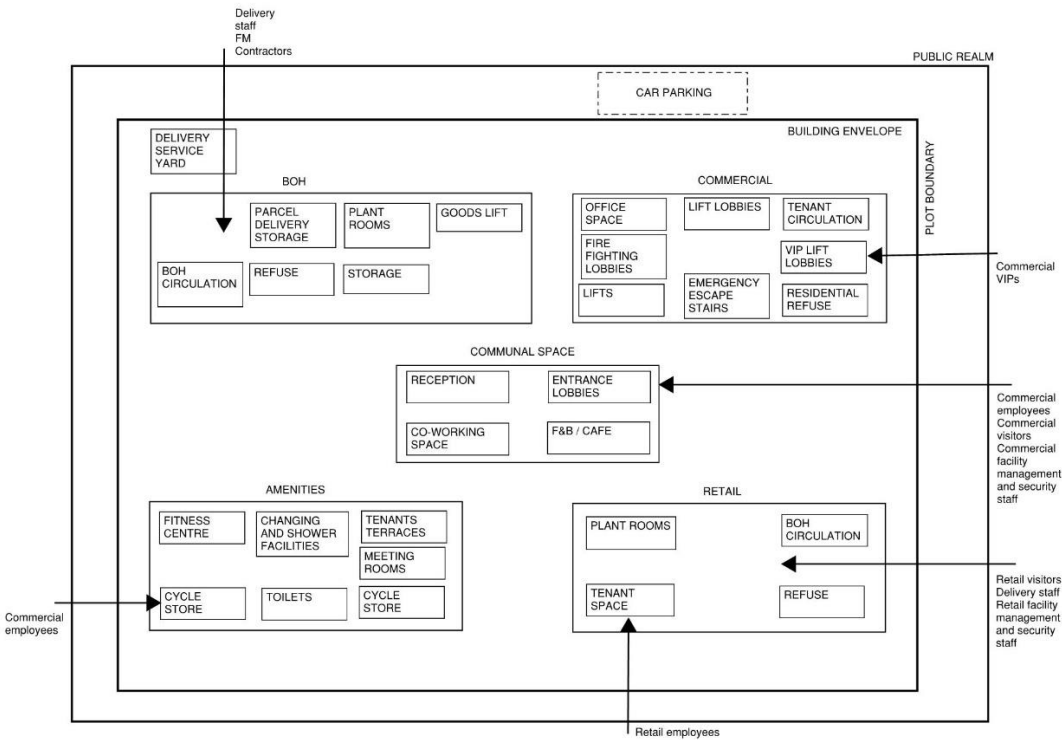


Figure 10. Commercial plots vulnerability relationships



Appendix D – Identify threats

Overview

The threat assessment provides an assessment of the crime and terrorism threats posed to the project. It will assess the key threats, including those identified by security stakeholders such as Police Designing Out Crime Officers, as well as intent and capability of the threat sources. It will also consider likely targets of the threats. The primary aims of the threat assessment are to identify the threats that are credible, thus forming the design basis threats (DBTs).

Threat assessment

A detailed threat assessment has been undertaken for the development. This can be found in Table 9.

A threat is a malicious action carried out by an individual or individuals (threat actor(s)) that has the potential to directly or indirectly have a negative impact on an asset or an organisation’s legitimate activities. It is derived from a consideration of intent and capability, where:

- Intent is the desire to create the threat. Not all threat actors wish to create all threats: a potential thief may not set out to harm people.
- Capability is the technical, logistical and organisational ability to mount an attack. For example, to create a credible threat of creating an explosion, an actor needs explosives which they must either obtain or create.

All threats are essentially criminal in nature and for the purpose of this assessment they are subdivided into terrorist and conventional crimes.

Information sources

The sources used within this assessment include: National Crime Agency, Centre for the Protection of National Infrastructure (CPNI), police crime data, media reports and workshops with the police / government authorities. Location specific crime data from the police can be found in Figure 11.

Threat analysis – Design basis threats

Design Basis Threats (DBTs) are those threats from the threat assessment that are deemed credible against the development – those threats rated very high to high. They will form the basis of any security needs or risk assessment and are outlined in Table 8 and in more detail within Table 9.

Additional to these credible threats, several “possible” threats exist and will be mitigated either in part / full by the security measures devised to address the credible threats.

Table 8. Design basis threats

Threat no.	Design Basis Threat	Threat no.	Design Basis Threat
T01	Explosive threat	T09	Burglary
T02	Vehicle as a weapon (VAW)	T10	Theft of (or from) a motor vehicle
T03	Close quarter attacks – solo	T11	Criminal damage and arson
T04	Close quarter attacks - coordinated	T12	Violent crime including attacks against the person and robbery.
T06	Insider threat (including radicalisation)	T13	Trespass
T08	Theft	T15	Antisocial behaviour and public order

Threat discussion

A number of DBTs warrant further discussion:

Explosive device (credible)

The threat from a person borne or placed device remains however, in the form of smaller devices being left in the public realm to target the crowd during events It is unlikely that an explosive attack would be directed towards the structures, rather against a crowd in the public realm. Whilst a vehicle borne device is possible, given the proximity of a category A transport hub in the form of Reading station, and the crowds it generates on certain occasions, it is considered that will be the more attractive and accessible target.

Vehicle As a Weapon (credible)

The threats of a Vehicle As a Weapon are deemed credible. All vehicle threats to the development have been considered and addressed within a separate Vehicle Threat Mitigation Strategy document (REP-2525046-02-DC-20190531-Station Hill HVM-Rev01).

Violent crime (credible)

The crime statistics indicate that violent crime is a very significant factor in area and that due diligence should be done to mitigate it where possible.

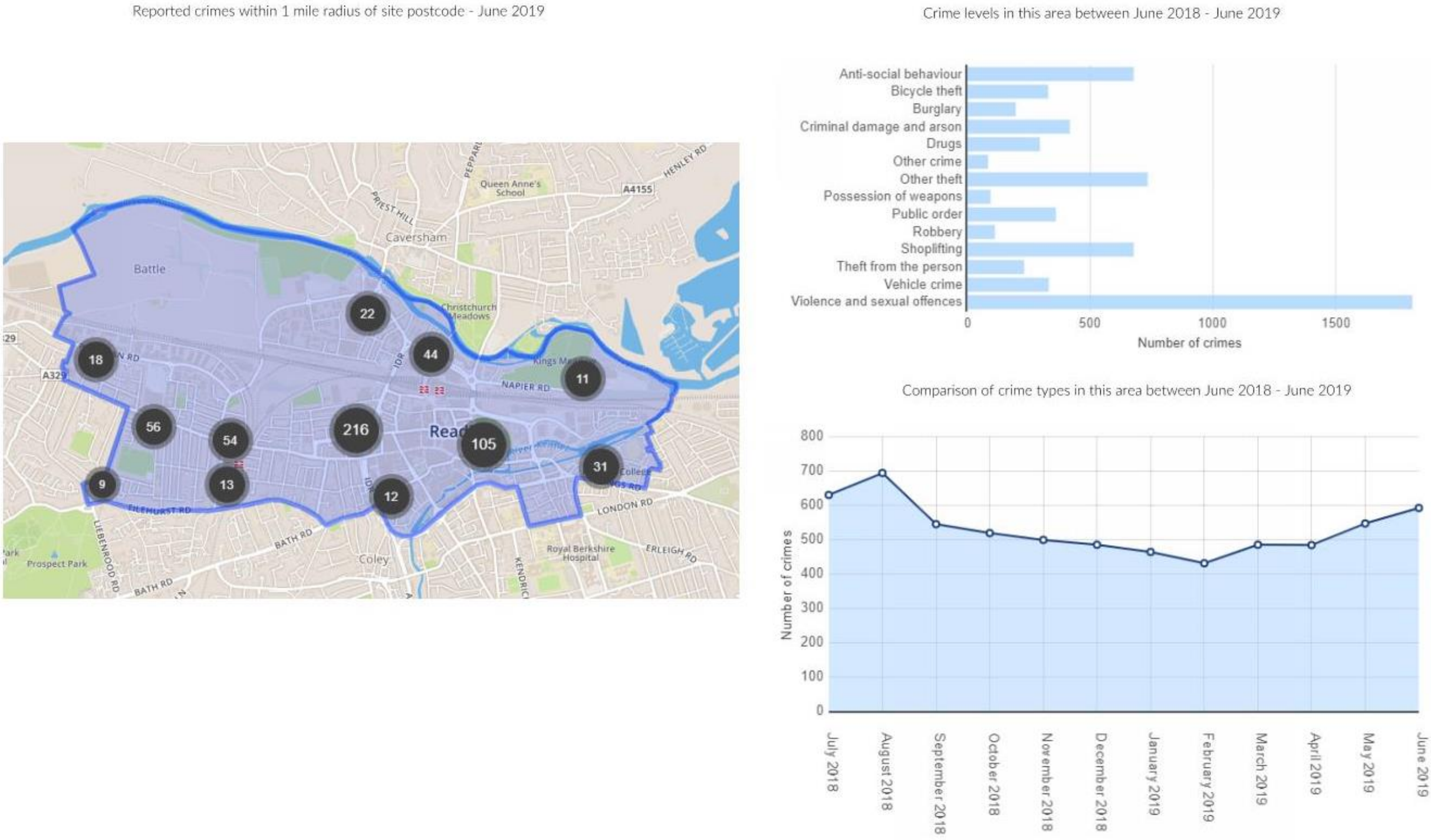
Theft (credible)

According to the available crime statistics, the presence of theft and similar offences feature prominently in the area and therefore merit specific attention. The activation of the public realm with retail and occasional events, combined with the daily throughput of pedestrians to and from the station and hence the increase of personal effects within the accessible areas, will increase the likelihood of theft in all its forms.

Anti-social behaviour (credible)

The crime statistics indicate that anti-social behaviour is a prominent challenge in the area. The activation of the public realm with retail and occasional events, combined with the daily thoroughfare of pedestrians to and from the station will increase the likelihood of anti-social behaviour and other threats that may manifest from an escalation of such behaviour. This will increase further on match days, due to the volume of exuberant match goers as they make their way to and from the station through the development.

Figure 11. Crime statistics



Source: Police UK

Table 9. Threat register

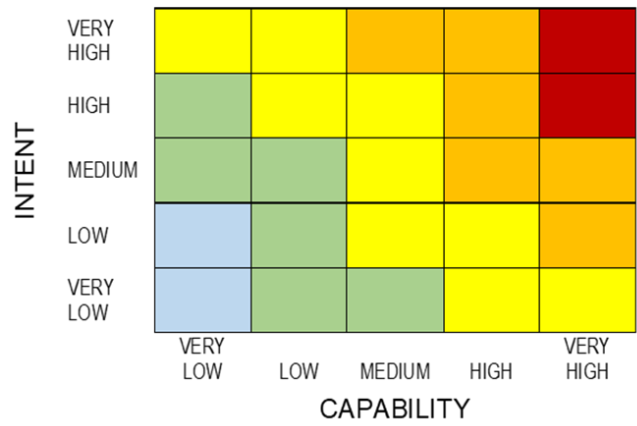
Threat no.	Threat	Source / threat actor	Summary comment	Targeting	Capability	Intent	Threat rating
Terrorism							
T01	Explosive devices	Transnational terrorist network or domestic self-radicalised cell, Radicalised individual	These can be delivered to their targets in vehicles, by post or by a person. May include suicide attacks. Note: Charge sizes will be determined in consultation with government / police security advisers should this be considered a credible threat to the development requiring mitigation within the scope of the project	For placed devices - spaces that provide access to structural elements, façade, crowded spaces. For suicide devices – spaces that would maximise casualties e.g. retail spaces; communal shared spaces. For postal devices – all user group.	HIGH	MED	HIGH
T02	Vehicle as a weapon (VAW)	Transnational terrorist network or domestic self-radicalised cell, Radicalised individual Mentally disturbed individual	An attack utilising a vehicle as a weapon to kill, maim or cause damage Note: vehicle type and attack speeds should be determined as part of the design development should this be considered a credible threat to the development requiring mitigation within the scope of the project (For vehicle borne improvised explosive devices see explosive devices).	Spaces that provide access to structural elements, façade, spaces with large groups / high density of people.	HIGH	MED	HIGH
T03	Close quarter attacks - solo	Radicalised individual Mentally disturbed individual	These can include attacks utilising firearms, knives or other hand-held weapons or corrosive substances. (For attacks including vehicles see VAW)	Crowded areas / high density of people inside and outside the property.	HIGH	MED	HIGH
T04	Close quarter attacks - coordinated	Transnational terrorist network or domestic self-radicalised cell	Well organised, coordinated attacks by multiple individuals utilising firearms, knives, hand-held weapons or corrosive substances. (For attacks including vehicles see VAW)	Crowded areas / high density of people inside and outside the property.	HIGH	HIGH	HIGH
T05	Chemical, biological, radiological and nuclear (CBRN)	Transnational terrorist network or domestic self-radicalised cell, Radicalised individual	An attack including the use of chemical, biological, radiological or nuclear material designed to infect / poison / contaminate individuals or groups. Note: Material type and quantities will be determined in consultation with government / police security advisers should this be considered a credible threat to the development requiring mitigation within the scope of the project.	Plant rooms and air intakes located in the building. Post rooms / goods receiving areas.	LOW	MED	LOW
T06	Insider threat (including radicalisation)	Organised crime, transnational terrorist network or domestic self-radicalised cell. Disgruntled or unethical employees. Existing employees.	Criminal or terrorist organisations may try to subvert individuals within, or with access to, an organisation who can provide “insider” information that helps to plan an attack on the organisation. Could be religious or politically based (e.g. right-wing extremists) Likely to be an indirect threat i.e. threat will manifest itself elsewhere with the development experiencing secondary impact of the threat through one of the other threat events. Malicious acts by existing or past employees for personal gain, resulting in a secondary impact on the asset / organisations reputational and/or financial status.	Individuals getting access to spaces and / or networks where commercially sensitive information is available (including research data) An organisations' reputation and financial situation.	HIGH	MED	HIGH

Threat no.	Threat	Source / threat actor	Summary comment	Targeting	Capability	Intent	Threat rating
			Accidental occurrences caused by an employee during the course of their daily duties that result in potential liability issues, financial loss and reputational damage for the organisation.				
			The presence of varied business environments within the development broadens the opportunity for organised crime and insider based threats to manifest.				
T07	Hoax	Political activist, Environmental activist, Individuals with personality disorder / mental health issues or disgruntled (former) employees.	Actions designed to disrupt or scare recipient establishment or individuals. This may be a verbal notification (e.g. via telephone) or a delivered object. Generally associated with explosive devices or CBRN. Note: This may be a criminal activity rather than terrorist. However, it has been used by terrorist groups in the past to initiate movement of people to a particular location.	User groups. Security and management staff, Commercial unit employees.	HIGH	LOW	MED
Conventional Crime							
T08	Theft	Opportunist or premeditated individual(s) or gangs, Organised gangs	All developments possess assets that are attractive to thieves. This new built development comprises of public domain, different forms of accommodation and retail (café) spaces which are all attractive. Pre-planned thefts will always be preceded by a reconnaissance and are likely to involve insider knowledge. This includes theft / loss / compromise of data as well as petty theft. Existing employees may conduct lower profile malicious acts, which in themselves have a lesser initial impact, but cumulatively result in a larger impact for the unit or organisation (such fraud, corruption, deception, theft, misappropriation etc).	Any spaces frequented by user groups or those areas containing high value possessions or attractive assets.	VERY HIGH	VERY HIGH	VERY HIGH
T09	Burglary	Opportunist or premeditated individual(s) or gangs, Organised gangs	All developments will possess assets that have high value which makes them attractive to thieves. Burglary is the theft or attempted theft where access is not authorised. Pre-planned burglaries will always be preceded by a reconnaissance and are likely to involve insider knowledge.	Areas containing equipment or possessions that are easily transportable.	VERY HIGH	VERY HIGH	VERY HIGH
T10	Theft of (or from) a motor vehicle	Opportunist or premeditated individual(s) or gangs, Organised gangs	Theft of vehicles for resale, or entertainment (joy ride). Damage to vehicles to steal contents. Theft from vehicles of personal items etc.	Transition area between road and building or from parked vehicles within the boundary of the building.	HIGH	HIGH	HIGH
T11	Criminal damage and arson	Opportunist or premeditated individual(s) or gangs	Attacks can be launched against the built environment itself, the things contained within it or vehicles using the car park / vehicle delivery yard. Threats will arise from individuals or groups. May be used to convey a message, express frustration or boredom, or take revenge. Can be manifestation of hate crime.	External façade of unprotected or unmonitored areas. Secluded, unmonitored areas.	VERY HIGH	HIGH	VERY HIGH

Threat no.	Threat	Source / threat actor	Summary comment	Targeting	Capability	Intent	Threat rating
T12	Violent crime including attacks against the person and robbery.	Aggressive individuals / organised gangs	Violence against the person most commonly occurs as an aggravating factor in cases such as theft, or as a result of intoxication or emotional instability. Attacks typically have a strong locational factor, such as occurring near crowded social areas; though those with robbery as the primary motive can occur in secluded places such as alleyways and stairwells where attackers are less likely to be detected. May happen in conjunction with other threats such as burglary. Can included theft with the use of force or a threat of force, sexual offence and can be manifestation of hate crime. Occasionally there can be aggravating factors, such as use of corrosive substance.	Secluded areas within the development, External areas accessible to passing population (building curtilage only).	VERY HIGH	HIGH	VERY HIGH
T13	Trespass	Opportunist individual(s) Urban explorers Planned gatherings	Generally, an opportunistic activity seeking access to areas where entry is not permitted for unauthorised users. May be premeditated as part of a hostile reconnaissance. Trespass also includes exceeding permitted usage, such as by riding a motor scooter on a footpath or vehicle disturbance.	All access points to the buildings. Spaces with areas of interest within.	VERY HIGH	LOW	HIGH
T14	Protest	Individuals or groups in vicinity of, or directly associated with development Could rise to other threats such as anti-social behaviour or violence	Legitimate or illegal protest activities with the deliberate intent of conveying a message. Peaceful protests may evolve into violent protests either through circumstance or if hijacked by others with the intent of causing a disturbance, Note: The speed of this threat could change, depending upon the profile of the organisation(s) that may occupy the development.	Spaces where a high density of people can occupy and act as a group for the purpose of gaining maximum exposure or publicity e.g. Car Park, roof tops.	HIGH	LOW	MED
T15	Antisocial behaviour and public order	Individuals or groups in vicinity of, or directly associated with development Could rise to other threats such as violent crime	Antisocial behaviour is that which falls short of criminal but is often intimidator and distressing for the victim(s). Public order is the criminal aspect of anti-social behaviour and covers everything from riots to an individual causing distress. The vast majority of public order offences are at the lower end of the scale. Antisocial behaviour and public order may arise around or within the buildings from legitimate users.	Building curtilage, car parks.	VERY HIGH	HIGH	VERY HIGH

Threat rating definitions and capability and intent criteria

Rating	Description	Capability	Intent
VERY HIGH	The threat source has very significant capability, declared intent and there exists strong, recent precedent of such actions, therefore a credible threat exists against assets.	There is potential for there to be multiple threat sources and for these to exist locally. Required resources (e.g. logistical, technical and financial) are easily / readily available. Threat source(s) have the required level of knowledge and expertise to carry out the threat event.	There is very significant evidence of the threat source's intent to carry out the threat. The threat source can expect very significant monetary, political or publicity gain. The type of threat event has been seen regularly.
HIGH	The threat source has significant capability, declared intent and there exists some limited precedent of such actions, therefore a credible threat exists against assets.	The threat sources are likely to exist locally. Required resources (e.g. logistical, technical and financial) are reasonably available. Threat source(s) have the required level of knowledge and expertise to carry out the threat event.	There is significant evidence of the threat source's intent to carry out the threat. The threat source can expect significant monetary, political or publicity gain. The type of threat event has been seen.
MEDIUM	The threat source has reasonable capability and there exists some limited precedent but no specific declared intent of targeting similar assets. A possible threat exists.	The threat sources may exist locally or regionally. There is limited availability of required resources (e.g. logistical, technical and financial). Threat source(s) have some of the required level of knowledge and expertise to carry out the threat event, or a reasonable level of training is required.	There is some evidence of the threat source's intent to carry out the threat. The threat source can expect moderate monetary, political or publicity gain. There is a reasonable level of history of this type of threat event.
LOW	The threat source has limited capability, with no precedent of targeting similar assets. The threat exists but is not probable.	The threat sources are unlikely to exist locally but may be nationally. There is very limited availability of required resources (eg logistical, technical and financial). Threat source(s) have a limited level of knowledge and expertise to carry out the threat event, or specialist training is required.	There is limited evidence but some implication of the threat source's intent to carry out the threat. The threat source can expect limited monetary, political or publicity gain. There is only limited history of this type of threat event.
VERY LOW	The threat source has very limited or no capability, and there exists no precedent of the threat targeting assets. It is highly unlikely a threat exists.	The threat sources are extremely unlikely to exist locally but possibly internationally. There is significantly limited / negligible availability of required resources (e.g. logistical, technical and financial). Threat source(s) have a negligible level of knowledge and expertise to carry out the threat event, or significant advanced technical training is required.	There is negligible or no evidence or implication of the threat source's intent to carry out the threat. The threat source can expect negligible monetary, political or publicity gain. There is extremely limited history of this type of threat event.

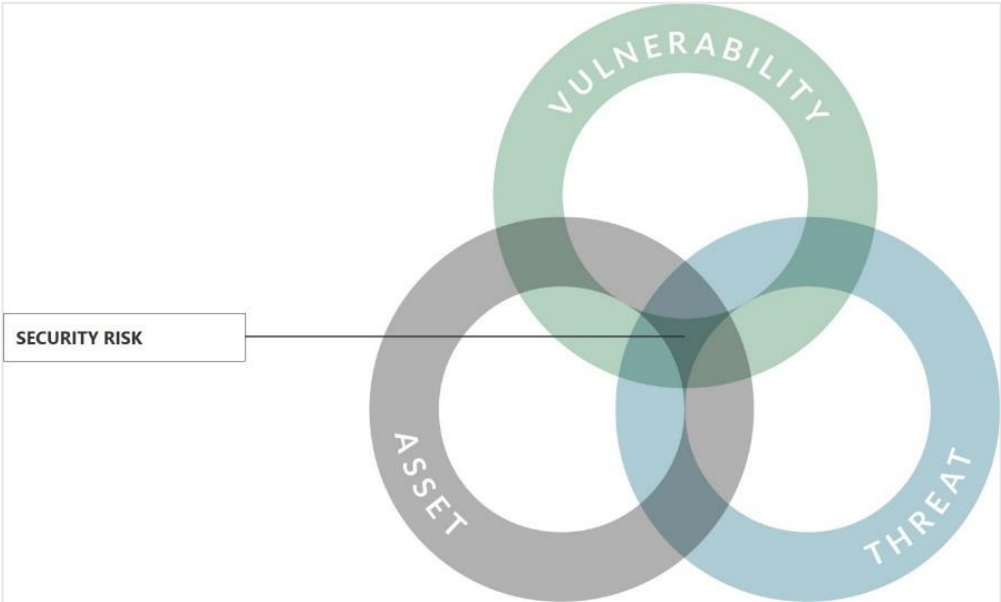


Appendix E - Identify and analyse risks

Overview

As defined in ISO 31000 (Risk Management-Principles and guidelines), a security risk exists where there is a likelihood that a threat can act upon a vulnerability and produce an impact. Hoare Lea security summarise this in Figure 11.

Figure 11. Security risk



Source: Hoare Lea

Risk evaluation

To determine the severity of the gross risk⁷ from a threat manifesting, an assessment is carried out, utilising likelihood and impact as the two influential factors:

- Likelihood is the chance of a given risk event occurring. It is linked to the attractiveness of a target to threat actors.
- Impact is the potential consequences of a risk event manifesting.

Whilst both factors in determining the magnitude of a risk, our approach is weighted towards impact since this will be the actual result of the risk materialising.

The detailed risk analysis is captured within the security risk register, Table 11. A qualitative approach has been adopted to assess the likelihood and impact of a risk (threat against a vulnerability).

In total, 34 risks, have been analysed for the development, the resulting categories are summarised in Table 10 and a high-level graphic indicating the relationship between risks and locations, Figure 4:

Table 10. Risk evaluation summary

Risk	No. of risks
VERY HIGH	3
HIGH	13
MEDIUM	14
LOW	4
VERY LOW	0

⁷ A gross risk represents the risk to the development prior to any risk treatment being imposed. After treatment, a net risk can be assessed.

Table 11. Risk register

Ser	Threat	Vulnerability	Likelihood	Description of impact (on asset)	Impact	Gross risk	Risk treatment (Sub-Operational Requirement)	DETER	DETECT	DELAY	RESPOND	RECOVER
R01	Explosive devices	Public realm Residential: Building envelope Commercial: Building envelope Retail: Building envelope	LOW	Irreparable damage and / or loss of major parts of the development and / or complete development Corporate impact on performance/objectives. Disruption to activity for extended period. International media attention	VERY HIGH	VERY HIGH	Provide physical measures to reduce impact of any blast (e.g. stand-off, glazing enhancements) as appropriate to determined charge size.					X
R02	Explosive devices	Residential: Entrance lobbies Commercial: Entrance lobbies	VERY LOW	Irreparable damage and / or loss of major parts of the development and / or complete development Corporate impact on performance/objectives. Disruption to activity for extended period. International media attention	VERY HIGH	VERY HIGH	Ensure security zones are established that support strategic security layering / defence in depth.	X		X		
							Provide physical barriers to all points of ingress and egress into the building through the building envelope.	X		X		
							Provide lighting throughout the development to support natural and electronic surveillance	X	X			
							Provide surveillance measures in all lobbies and reception areas.	X	X		X	
							Ensure security processes and procedures including security management plan, incident management and visitor, guest and contractor access approval.				X	X
							Provide command and control facilities to coordinate response and operational management.		X		X	X
R03	Vehicle as a weapon (VAW) ⁸	Public realm Car parks Residential: Building envelope Commercial: Building envelope Retail: Building envelope	HIGH	Serious injuries, inability to work, Significant Damage to reputation National media attention Major impact on performance / objectives.	HIGH	VERY HIGH	All vehicle threats to the development have been considered and addressed within a separate Vehicle Threat Mitigation Strategy document (REP-2525046-02-DC-20190531-Station Hill HVM-Rev01).					
R04	Vehicle as a weapon (VAW)	Residential: Entrance lobbies	LOW	Serious injuries, inability to work, Significant Damage to reputation	HIGH	HIGH	All vehicle threats to the development have been considered and addressed within a separate Vehicle Threat Mitigation Strategy document (REP-2525046-02-DC-20190531-Station Hill HVM-Rev01).					

⁸ Requirements for crash rated products to be determined following discussions with Thames Valley Police Counter Terrorism Security Adviser

Ser	Threat	Vulnerability	Likelihood	Description of impact (on asset)	Impact	Gross risk	Risk treatment (Sub-Operational Requirement)	DETER	DETECT	DELAY	RESPOND	RECOVER
		Commercial: Entrance lobbies Retail: Tenant space		National media attention Major impact on performance / objectives.								
R05	Close quarter attacks – solo	Public realm Car parking	LOW	Serious injuries, inability to work, Significant Damage to reputation National media attention Major impact on performance / objectives.	HIGH	HIGH	Ensure security zones are established that support strategic security layering / defence in depth.	X		X		
							Provide a physical barrier to the car parking.	X		X		
							Provide lighting throughout the development to support natural and electronic surveillance	X	X			
							Provide surveillance to monitor activity in the public realm and car parking.	X	X		X	
							Provide command and control facilities to coordinate response and operational management.		X		X	X
							Ensure security processes and procedures including security management plan, incident management and visitor, guest and contractor access approval.				X	X
R06	Close quarter attacks – solo	Residential: Entrance lobbies Reception Commercial: Entrance lobbies Reception	VERY LOW	Serious injuries, inability to work, Significant Damage to reputation National media attention Major impact on performance / objectives.	HIGH	HIGH	Ensure security zones are established that support strategic security layering / defence in depth.	X		X		
							Provide physical barriers to all points of ingress and egress into the building through the building envelope.	X		X		
							Provide lighting throughout the development to support natural and electronic surveillance	X	X			
							Provide surveillance measures in all lobbies and reception areas.	X	X		X	
							Provide ability for staff to raise alarm.		X		X	X
							Provide command and control facilities to coordinate response and operational management.		X		X	X
R07	Close quarter attacks – solo	Residential: Lift lobbies	VERY LOW	Serious injuries, inability to work,	HIGH	HIGH	Provide control of access between security zones in order to control and/or deter and delay access.	X	X	X		

Ser	Threat	Vulnerability	Likelihood	Description of impact (on asset)	Impact	Gross risk	Risk treatment (Sub-Operational Requirement)	DETER	DETECT	DELAY	RESPOND	RECOVER
		Lifts Circulation Communal / shared amenities Commercial: Lift lobbies Lifts Circulation VIP lift lobbies F&B / Cafe		Significant Damage to reputation National media attention Major impact on performance / objectives.			Provide a minimum of two lines of control to gain access to all cores and circulation.	X		X		
							Provide control of access to all lift lobbies, lifts, circulation areas, VIP lift lobbies and amenities.	X		X		
							Provide vertical and horizontal compartmentalisation of floors.	X		X		
							Provide dynamic lock-down capability (including cores).			X	X	X
							Provide ability for staff to raise alarm.		X		X	X
							Provide command and control facilities to coordinate response and operational management.		X		X	X
R08	Close quarter attacks - solo	Residential: Delivery service yard BOH circulation Commercial: Delivery service yard BOH circulation	VERY LOW	Substantial, but recoverable loss of resource Potential loss: £10,000s Long term loss of future user groups.	MED	LOW	Ensure security zones are established that support strategic security layering / defence in depth.	X	X	X		
							Provide physical barrier to the delivery service yards.	X		X		
							Provide control of access between security zones in order to control and/or deter and delay access.	X	X	X		
							Provide lighting throughout the development to support natural and electronic surveillance	X	X			
							Provide control of access to the BOH circulation.	X		X		
							Provide ability for audio and visual communication from key operational access-controlled points, such as, but not limited to the delivery service yards.		X		X	
							Provide surveillance to monitor activity within the delivery service yards and BOH circulation.	X	X		X	
							Provide command and control facilities to coordinate response and operational management.		X		X	X
							Ensure security processes and procedures including security management plan, incident management and visitor, guest and contractor access approval.				X	X
R09		Public realm Car parking	LOW	Serious injuries, inability to work,	HIGH	HIGH	Ensure security zones are established that support strategic security layering / defence in depth.	X		X		

Ser	Threat	Vulnerability	Likelihood	Description of impact (on asset)	Impact	Gross risk	Risk treatment (Sub-Operational Requirement)	DETER	DETECT	DELAY	RESPOND	RECOVER
	Close quarter attacks - coordinated			Significant Damage to reputation National media attention Major impact on performance / objectives.			Provide a physical barrier to the car parking.	X		X		
							Provide lighting throughout the development to support natural and electronic surveillance	X	X			
							Provide surveillance to monitor activity in the public realm and car parking.	X	X		X	
							Provide command and control facilities to coordinate response and operational management.		X		X	X
							Ensure security processes and procedures including security management plan, incident management and visitor, guest and contractor access approval.				X	X
R10	Close quarter attacks - coordinated	Residential: Entrance lobbies Reception Commercial: Entrance lobbies Reception F&B / Cafe	VERY LOW	Serious injuries, inability to work, Significant Damage to reputation National media attention Major impact on performance / objectives.	HIGH	HIGH	Ensure security zones are established that support strategic security layering / defence in depth.	X		X		
							Provide physical barriers to all points of ingress and egress into the building through the building envelope.	X		X		
							Provide lighting throughout the development to support natural and electronic surveillance	X	X			
							Provide surveillance measures in all lobbies, reception areas and the cafe.	X	X		X	
R11	Close quarter attacks - coordinated	Residential: Lift lobbies Lifts Circulation Communal / shared amenities Commercial: Lift lobbies Lifts Circulation VIP lift lobbies	VERY LOW	Serious injuries, inability to work, Significant Damage to reputation National media attention Major impact on performance / objectives.	HIGH	HIGH	Provide physical barriers between security zones to control access and deter or delay access.	X	X	X		
							Provide control of access to all lift lobbies, lifts, circulation areas, VIP lift lobbies and amenities.	X		X		
							Provide vertical and horizontal compartmentalisation of floors.	X		X		
							Provide dynamic lock-down capability (including cores).			X	X	X
							Provide ability for staff to raise alarm.		X		X	X
							Provide command and control facilities to coordinate response and operational management.		X		X	X
R12	Close quarter attacks - coordinated	Residential: Delivery service yard BOH circulation	VERY LOW	Substantial, but recoverable loss of resource Potential loss: £10,000s	MED	LOW	Ensure security zones are established that support strategic security layering / defence in depth.	X	X	X		
							Provide physical barrier to the delivery service yards.	X		X		

Ser	Threat	Vulnerability	Likelihood	Description of impact (on asset)	Impact	Gross risk	Risk treatment (Sub-Operational Requirement)	DETER	DETECT	DELAY	RESPOND	RECOVER
		Commercial: Delivery service yard BOH circulation		Long term loss of future user groups.			Provide lighting throughout the development to support natural and electronic surveillance	X	X			
							Provide control of access to the BOH circulation.	X		X		
							Provide ability for audio and visual communication from key operational access-controlled points, such as, but not limited to the delivery service yards.	X		X	X	
							Provide surveillance to monitor activity within the delivery service yards and BOH circulation.	X	X		X	
							Provide command and control facilities to coordinate response and operational management.		X		X	X
							Ensure security processes and procedures including security management plan, incident management and visitor, guest and contractor access approval.				X	X
R13	Insider threat (including radicalisation)	Residential: Reception Delivery service yard Plant rooms BOH circulation Commercial: Reception Delivery service yard Plant rooms BOH circulation Retail: BOH circulation	HIGH	Substantial, but recoverable loss of resource Potential loss: £10,000s Long term loss of future user groups.	MED	HIGH	Ensure security zones are established that support strategic security layering / defence in depth.	X	X	X		
							Provide surveillance to receptions, delivery service yards and BOH circulation.	X	X		X	
							Provide surveillance to monitor access to all plant rooms.		X		X	
							Provide lighting throughout the development to support natural and electronic surveillance	X	X			
							Provide control of access to the BOH circulation and plant rooms.	X		X		
							Provide physical barrier to the delivery service yards.	X		X		
							Secure key cabinets and management protocols will be required.	X		X		
							Ensure security processes and procedures including security management plan, incident management and visitor, guest and contractor access approval.				X	X
							Provide command and control facilities to coordinate response and operational management.		X		X	X
							Provide associated infrastructure to support electronic security systems.		X		X	X
R14	Theft	Public Realm Car parking	VERY HIGH	Recoverable short-term disruption.	LOW	MED	Ensure security zones are established that support strategic security layering / defence in depth.	X	X	X		

Ser	Threat	Vulnerability	Likelihood	Description of impact (on asset)	Impact	Gross risk	Risk treatment (Sub-Operational Requirement)	DETER	DETECT	DELAY	RESPOND	RECOVER
				Potential loss: £1,000s Possible moderate injury if the risk rises to violence. Adverse local media attention Some impact on reputation.			Provide physical barriers to the car parking.	X		X		
							Provide ability to detect unauthorised movement within or between security zones.		X		X	
							Provide lighting throughout the development to support natural and electronic surveillance	X	X			
							Provide surveillance to monitor activity in the public realm and car parking.	X	X		X	
							Ensure security processes and procedures including security management plan, incident management and visitor, guest and contractor access approval.				X	X
							Provide command and control facilities to coordinate response and operational management.		X		X	X
							Provide associated infrastructure to support electronic security systems.		X		X	X
R15	Theft	Residential: Entrance lobbies Reception Post Commercial: Entrance lobbies Reception F&B / Café Co-working space Meeting rooms	VERY HIGH	Recoverable short-term disruption. Potential loss: £1,000s Possible moderate injury if the risk rises to violence. Adverse local media attention Some impact on reputation.	LOW	MED	Ensure security zones are established that support strategic security layering / defence in depth.	X	X	X		
							Provide vertical and horizontal compartmentalisation of floors.	X		X		
							Provide control of access between security zones in order to control and/or deter and delay access	X	X	X		
							Provide surveillance to the post, all entrance lobbies, receptions, co-working space, café and meeting rooms.	X	X		X	
							Provide lighting throughout the development to support natural and electronic surveillance	X	X			
							Provide physical barriers to all points of ingress and egress into the building through the building envelope.	X		X		
							Provide control of access to the post, co-working space and meeting rooms.	X		X		
							Ensure security processes and procedures including security management plan, incident management and visitor, guest and contractor access approval.				X	X
							Provide command and control facilities to coordinate response and operational management.		X		X	X

Ser	Threat	Vulnerability	Likelihood	Description of impact (on asset)	Impact	Gross risk	Risk treatment (Sub-Operational Requirement)	DETER	DETECT	DELAY	RESPOND	RECOVER
R16	Theft	Residential: Lift lobbies Lifts Goods lifts Circulation Communal / shared amenities Commercial: Lift lobbies Lifts Circulation VIP lift lobbies	MED	Recoverable short-term disruption. Potential loss: £1,000s Possible moderate injury if the risk rises to violence. Adverse local media attention Some impact on reputation.	LOW	MED	Ensure security zones are established that support strategic security layering / defence in depth.	X	X	X		
							Provide vertical and horizontal compartmentalisation of floors.	X		X		
							Provide control of access to all lift lobbies, lifts, circulation areas, VIP lift lobbies and amenities.	X		X		
							Provide surveillance to all lift lobbies, lifts, goods lifts, VIP lifts lobbies, circulation and communal / shared amenities.	X	X		X	
							Provide lighting throughout the development to support natural and electronic surveillance	X	X			
							Provide command and control facilities to coordinate response and operational management.		X		X	X
							Provide associated infrastructure to support electronic security systems.		X		X	X
R17	Theft	Commercial: Office space	MED	Recoverable short-term disruption. Potential loss: £1,000s Possible moderate injury if the risk rises to violence. Adverse local media attention Some impact on reputation.	LOW	MED	Provide vertical and horizontal compartmentalisation of floors.	X		X		
							Provide control of access to the office space (containment only)	X		X		
							Provide surveillance to monitor access to all office spaces.	X	X		X	
							Ensure security processes and procedures including security management plan, incident management and visitor, guest and contractor access approval.				X	X
R18	Theft	Residential: Delivery service yard BOH circulation Storage Cycle storage Plant rooms Commercial: Delivery service yard BOH circulation Storage Cycle storage Plant rooms	VERY HIGH	Recoverable short-term disruption. Potential loss: £1,000s Possible moderate injury if the risk rises to violence. Adverse local media attention Some impact on reputation.	LOW	MED	Provide physical barriers to spaces containing high value items (EG. Cycle storage etc).	X		X		
							Provide physical barrier to the delivery service yards.	X		X		
							Provide control of access to the BOH circulation and plant rooms.	X		X		
							Provide surveillance to the delivery service yard, storage, cycle storage and BOH circulation.	X	X		X	
							Provide lighting throughout the development to support natural and electronic surveillance	X	X			
							Provide associated infrastructure to support electronic security systems.		X		X	X

Ser	Threat	Vulnerability	Likelihood	Description of impact (on asset)	Impact	Gross risk	Risk treatment (Sub-Operational Requirement)	DETER	DETECT	DELAY	RESPOND	RECOVER
							Provide command and control facilities to coordinate response and operational management.		X		X	X
							Ensure security processes and procedures including security management plan, incident management and visitor, guest and contractor access approval.				X	X
R19	Theft of (or from) a motor vehicle	Public realm Car parks	VERY HIGH	Substantial, but recoverable loss of resource Potential loss: £10,000s Long term loss of future user groups.	MED	HIGH	Ensure security zones are established that support strategic security layering / defence in depth.	X		X		
							Provide a physical barrier to the car parking.	X		X		
							Provide lighting throughout the development to support natural and electronic surveillance	X	X			
							Provide surveillance to monitor activity in the public realm and car parking.	X	X		X	
							Provide command and control facilities to coordinate response and operational management.		X		X	X
							Ensure security processes and procedures including security management plan, incident management and visitor, guest and contractor access approval.				X	X
							Provide associated infrastructure to support electronic security systems.		X		X	X
R20	Theft of (or from) a motor vehicle	Residential: Delivery service yard Commercial: Delivery service yard	VERY HIGH	Substantial, but recoverable loss of resource Potential loss: £10,000s Long term loss of future user groups.	MED	HIGH	Ensure security zones are established that support strategic security layering / defence in depth.	X		X		
							Provide a physical barrier to the delivery service yard.	X		X		
							Provide lighting throughout the development to support natural and electronic surveillance	X	X			
							Provide surveillance to monitor activity in the delivery service yard.	X	X		X	
							Provide command and control facilities to coordinate response and operational management.		X		X	X
							Ensure security processes and procedures including security management plan, incident management and visitor, guest and contractor access approval.				X	X
							Provide associated infrastructure to support electronic security systems.		X		X	X

Ser	Threat	Vulnerability	Likelihood	Description of impact (on asset)	Impact	Gross risk	Risk treatment (Sub-Operational Requirement)	DETER	DETECT	DELAY	RESPOND	RECOVER
R21	Burglary	Residential: Cycle storage Storage rooms Commercial: Cycle storage Storage rooms Retail: Retail tenant space ⁹	HIGH	Recoverable short-term disruption. Potential loss: £1,000s Possible moderate injury if the risk rises to violence. Adverse local media attention Some impact on reputation.	LOW	MED	Ensure security zones are established that support strategic security layering / defence in depth.	X	X	X		
							Provide ability to detect unauthorised movement within or between security zones.		X		X	
							Provide physical barrier between security zones in to control access and to deter or delay access.	X	X	X		
							Provide physical barriers to all points of ingress and egress into the building through the building envelope.	X		X		
							Provide ability to detect intrusion to restricted areas.	X	X		X	
							Provide control of access to storage rooms.	X		X		
							Provide surveillance to monitor activity within the cycle storage.	X	X		X	
							Provide surveillance to monitor access to storage rooms, including, but not limited to the cycle store.	X	X		X	
							Provide lighting throughout the development to support natural and electronic surveillance	X	X			
							Provide command and control facilities to coordinate response and operational management.		X		X	X
							Ensure security processes and procedures including security management plan, incident management and visitor, guest and contractor access approval.				X	X
R22	Burglary	Residential: Apartments Gym Commercial: Office space	HIGH	Recoverable short-term disruption. Potential loss: £1,000s Possible moderate injury if the risk rises to violence. Adverse local media attention Some impact on reputation.	LOW	MED	Ensure security zones are established that support strategic security layering / defence in depth.	X	X	X		
							Ensure security zones are established that support strategic security layering / defence in depth.	X	X	X		
							Provide vertical and horizontal compartmentalisation of floors.	X		X		

⁹ Measures within these spaces are the responsibility of the owner / tenant

Ser	Threat	Vulnerability	Likelihood	Description of impact (on asset)	Impact	Gross risk	Risk treatment (Sub-Operational Requirement)	DETER	DETECT	DELAY	RESPOND	RECOVER
		Parcel delivery space Fitness centre					Provide control of access to the gym, parcel delivery space, apartments.	X		X		
							Provide control of access to the office space (containment only)	X		X		
							Provide surveillance to the access to the fitness centre, parcel delivery, office space gym and apartments.	X	X		X	
							Provide lighting throughout the development to support natural and electronic surveillance.	X	X			
							Provide command and control facilities to coordinate response and operational management.		X		X	X
R23	Burglary	Residential: Delivery service yard Plant rooms Commercial: Delivery service yard Plant rooms	HIGH	Substantial, but recoverable loss of resource Potential loss: £10,000s Long term loss of future user groups.	MED	HIGH	Provide ability to detect intrusion to restricted areas.	X	X			
							Provide surveillance to monitor access to all plant rooms.		X		X	
							Provide physical barrier to the delivery service yards and plant rooms.	X		X		
							Provide lighting throughout the development to support natural and electronic surveillance	X	X			
							Provide surveillance to the delivery service yard.	X	X		X	
							Ensure security processes and procedures including security management plan, incident management and visitor, guest and contractor access approval.				X	X
							Provide associated infrastructure to support electronic security systems.		X		X	X
R24	Criminal damage and arson	Public realm Car parking Residential: Building envelope Commercial: Building envelope Retail:	VERY HIGH	Recoverable short-term disruption. Potential loss: £1,000s Possible moderate injury if the risk rises to violence. Adverse local media attention Some impact on reputation.	LOW	MED	Provide a physical barrier to the car parking.	X		X		
							Provide lighting throughout the development to support natural and electronic surveillance.	X	X		X	
							Provide surveillance to monitor activity in the public realm and car parking.	X	X		X	
							Provide command and control facilities to coordinate response and operational management.		X		X	X

Ser	Threat	Vulnerability	Likelihood	Description of impact (on asset)	Impact	Gross risk	Risk treatment (Sub-Operational Requirement)	DETER	DETECT	DELAY	RESPOND	RECOVER
		Building envelope					Ensure security processes and procedures including security management plan, incident management and visitor, guest and contractor access approval.				X	X
R25	Criminal damage and arson	Residential: Entrance lobbies Reception Commercial: Entrance lobbies Reception F&B / Café Co-working space	HIGH	Recoverable short-term disruption. Potential loss: £1,000s Possible moderate injury if the risk rises to violence. Adverse local media attention Some impact on reputation.	LOW	MED	Ensure security zones are established that support strategic security layering / defence in depth.	X	X	X		
							Provide vertical and horizontal compartmentalisation of floors.	X		X		
							Provide control of access between security zones in to control access and to deter or delay access.	X	X	X		
							Provide surveillance to all entrance lobbies, receptions, co-working space, café and meeting rooms.	X	X		X	
							Provide lighting throughout the development to support natural and electronic surveillance.	X	X		X	
							Provide physical barriers to all points of ingress and egress into the building through the building envelope.	X		X		
							Provide control of access to the post, co-working space and meeting rooms.	X		X		
							Ensure security processes and procedures including security management plan, incident management and visitor, guest and contractor access approval.				X	X
							Provide command and control facilities to coordinate response and operational management.		X		X	X
R26	Criminal damage and arson	Residential: Lift lobbies Lifts Goods lifts Circulation Communal / shared amenities Commercial: Lift lobbies Lifts Circulation VIP lift lobbies	MED	Recoverable short-term disruption. Potential loss: £1,000s Possible moderate injury if the risk rises to violence. Adverse local media attention Some impact on reputation.	LOW	MED	Ensure security zones are established that support strategic security layering / defence in depth.	X	X	X		
							Provide vertical and horizontal compartmentalisation of floors.	X		X		
							Provide control of access to all lift lobbies, lifts, circulation areas, VIP lift lobbies and amenities.	X		X		
							Provide surveillance to all lift lobbies, lifts, goods lifts, VIP lifts lobbies, circulation and communal / shared amenities.	X	X		X	
							Provide lighting throughout the development to support natural and electronic surveillance.	X	X			
							Provide command and control facilities to coordinate response and operational management.		X		X	X

Ser	Threat	Vulnerability	Likelihood	Description of impact (on asset)	Impact	Gross risk	Risk treatment (Sub-Operational Requirement)	DETER	DETECT	DELAY	RESPOND	RECOVER
							Provide associated infrastructure to support electronic security systems.		X		X	X
R27	Criminal damage and arson	Residential: Delivery service yard Plant rooms BOH circulation Refuse Commercial: Delivery service yard Plant rooms BOH circulation Refuse	HIGH	Substantial, but recoverable loss of resource Potential loss: £10,000s Long term loss of future user groups.	MED	HIGH	Ensure security zones are established that support strategic security layering / defence in depth.	X		X		
							Provide a physical barrier to the delivery service yard.	X		X		
							Provide lighting throughout the development to support natural and electronic surveillance.	X	X		X	
							Provide surveillance to monitor activity in the delivery service yard.	X	X		X	
							Provide surveillance to monitor access to all plant rooms.		X		X	
							Provide command and control facilities to coordinate response and operational management.		X		X	X
							Ensure security processes and procedures including security management plan, incident management and visitor, guest and contractor access approval.				X	X
							Provide associated infrastructure to support electronic security systems.		X		X	X
R28	Violent crime including attacks against the person and robbery.	Public realm Car parking	HIGH	Recoverable short-term disruption. Potential loss: £1,000s Possible moderate injury if the risk rises to violence. Adverse local media attention Some impact on reputation.	LOW	MED	Ensure security zones are established that support strategic security layering / defence in depth.	X		X		
							Provide a physical barrier to the car parking.	X		X		
							Provide lighting throughout the development to support natural and electronic surveillance.	X	X		X	
							Provide surveillance to monitor activity in the public realm and car parking.	X	X		X	
							Provide command and control facilities to coordinate response and operational management.		X		X	X
							Ensure security processes and procedures including security management plan, incident management and visitor, guest and contractor access approval.				X	X
							Provide associated infrastructure to support electronic security systems.		X		X	X

Ser	Threat	Vulnerability	Likelihood	Description of impact (on asset)	Impact	Gross risk	Risk treatment (Sub-Operational Requirement)	DETER	DETECT	DELAY	RESPOND	RECOVER
R29	Violent crime including attacks against the person and robbery.	Residential: Entrance lobbies Reception Commercial: Entrance lobbies Reception F&B / Café Co-working space Meeting rooms	MED	Recoverable short-term disruption. Potential loss: £1,000s Possible moderate injury if the risk rises to violence. Adverse local media attention Some impact on reputation.	LOW	MED	Ensure security zones are established that support strategic security layering / defence in depth.	X	X	X		
							Provide vertical and horizontal compartmentalisation of floors.	X		X		
							Provide physical barrier between security zones in to control access and to deter or delay access.	X	X	X		
							Provide surveillance to the post, all entrance lobbies, receptions, co-working space, café and meeting rooms.	X	X		X	
							Provide lighting throughout the development to support natural and electronic surveillance.	X	X			
							Provide physical barriers to all points of ingress and egress into the building through the building envelope.	X		X		
							Provide control of access to the post, co-working space and meeting rooms.	X		X		
							Ensure security processes and procedures including security management plan, incident management and visitor, guest and contractor access approval.				X	X
							Provide command and control facilities to coordinate response and operational management.		X		X	X
R30	Violent crime including attacks against the person and robbery.	Residential: Lift lobbies Lifts Goods lifts Circulation Communal / shared amenities Commercial: Lift lobbies Lifts Circulation VIP lift lobbies	MED	Recoverable short-term disruption. Potential loss: £1,000s Possible moderate injury if the risk rises to violence. Adverse local media attention Some impact on reputation.	LOW	MED	Ensure security zones are established that support strategic security layering / defence in depth.	X	X	X		
							Provide vertical and horizontal compartmentalisation of floors.	X		X		
							Provide control of access to all lift lobbies, lifts, circulation areas, VIP lift lobbies and amenities.	X		X		
							Provide surveillance to all lift lobbies, lifts, goods lifts, VIP lifts lobbies, circulation and communal / shared amenities.	X	X		X	
							Provide lighting throughout the development to support natural and electronic surveillance.	X	X			
							Provide command and control facilities to coordinate response and operational management.		X		X	X

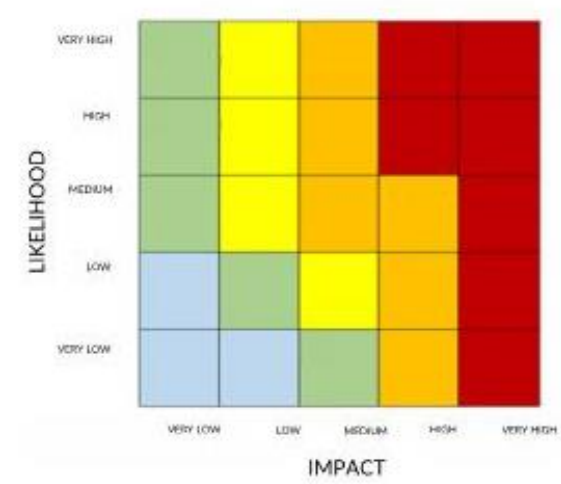
Ser	Threat	Vulnerability	Likelihood	Description of impact (on asset)	Impact	Gross risk	Risk treatment (Sub-Operational Requirement)	DETER	DETECT	DELAY	RESPOND	RECOVER
							Provide associated infrastructure to support electronic security systems.		X		X	X
R31	Violent crime including attacks against the person and robbery.	Residential: Delivery service yard BOH circulation Commercial: Delivery service yard BOH circulation	HIGH	Recoverable short-term disruption. Potential loss: £1,000s Possible moderate injury if the risk rises to violence. Adverse local media attention Some impact on reputation.	LOW	MED	Ensure security zones are established that support strategic security layering / defence in depth.	X		X		
							Provide a physical barrier to the delivery service yard.	X		X		
							Provide lighting throughout the development to support natural and electronic surveillance.	X	X			
							Provide surveillance to monitor activity in the delivery service yard.	X	X		X	
							Provide command and control facilities to coordinate response and operational management.		X		X	X
							Ensure security processes and procedures including security management plan, incident management and visitor, guest and contractor access approval.				X	X
							Provide associated infrastructure to support electronic security systems.		X		X	X
R32	Trespass	All Vulnerabilities (except public realm)	VERY HIGH	Substantial, but recoverable loss of resource Potential loss: £10,000s Long term loss of future user groups.	MED	HIGH	Ensure security zones are established that support strategic security layering / defence in depth.	X	X	X		
							Provide vertical and horizontal compartmentalisation of floors.	X		X		
							Provide control of access between security zones in to control access and to deter or delay access.	X	X	X		
							Provide physical barriers to all points of ingress and egress into the building through the building envelope.	X		X		
							Provide ability to detect unauthorised movement within or between security zones.		X		X	
							Provide a minimum of two lines of control to gain access to all oces and circulation.	X		X		
							Provide lighting throughout the development to support natural and electronic surveillance.	X	X			
							Provide surveillance to the public realm and throughout the development.	X	X		X	
							Provide control of access to all lift lobbies, lifts, circulation areas, VIP lift lobbies and amenities.	X		X		

Ser	Threat	Vulnerability	Likelihood	Description of impact (on asset)	Impact	Gross risk	Risk treatment (Sub-Operational Requirement)	DETER	DETECT	DELAY	RESPOND	RECOVER
							Provide ability for audio and visual communication from key operational access-controlled points, such as, but not limited to the delivery service yards, car park entrances, cycle storage entrances and main entrances.		X		X	
							Provide command and control facilities to coordinate response and operational management.		X		X	X
							Ensure security processes and procedures including security management plan, incident management and visitor, guest and contractor access approval.				X	X
							Provide associated infrastructure to support electronic security systems.		X		X	X
R33	Antisocial behaviour and public order	Public realm	VERY HIGH	Minor inconvenience. Potential disruption of activity. Potential rise to other threats such as theft or violence.	VERY LOW	LOW						
R34	Antisocial behaviour and public order	Residential: Entrance lobbies Reception Lift lobbies Lifts Goods lifts Circulation Communal / shared amenities Delivery service yard BOH circulation Commercial: Entrance lobbies Reception F&B / Café Lift lobbies Lifts Circulation VIP lift lobbies	HIGH	Minor inconvenience. Potential disruption of activity. Potential rise to other threats such as theft or violence.	VERY LOW	LOW						

Ser	Threat	Vulnerability	Likelihood	Description of impact (on asset)	Impact	Gross risk	Risk treatment (Sub-Operational Requirement)	DETER	DETECT	DELAY	RESPOND	RECOVER
		Delivery service yard BOH circulation										

Qualitative likelihood and impact ratings tables

Grading	Likelihood	Impact rating	Categories of impact and typical examples			
			Damage / loss to assets	Disruption to activity, loss of revenue	Harm to people	Reputation
VERY HIGH	So frequent as to be commonplace	VERY HIGH	Irreparable damage and / or loss of major parts of the development and / or complete development	Irreversible or substantial long-term service disruption. Irrecoverable substantial loss of income. Corporate impact on performance/objectives. Disruption to activity for extended period.	Multiple fatalities and serious injuries.	International media attention Government intervention/catastrophic damage to reputation. Development forced to close.
HIGH	Quarterly would not be uncommon	HIGH	(£100,000s)	Recoverable widespread or substantial service disruption. Major impact on performance/ objectives. Significant disruption to activity, possibly causing cancellation.	Single fatality, multiple serious injuries, disability.	Adverse comments from auditors/ significant damage to reputation/ National media attention Loss of major donors/sponsors as applicable Senior management forced to change.
MEDIUM	Once a year would not be uncommon	MEDIUM	(£10,000s)	Substantial, but recoverable loss of resource. Longer closure of a development, forcing a move to a temporary facility.	Serious injuries, inability to work.	Long term loss of future user groups.
LOW	Once a decade would not be uncommon	LOW	(£1000s)	Recoverable, localised, short term service disruption. Limited/local impact on performance/objectives. Temporary closure of an entrance or facility, absorbable in current capacity.	Moderate yet recoverable injury, harm or work absence. Multiple minor injuries.	Adverse local media attention/ service user complaints. Some impact on reputation. Major adverse publicity.
VERY LOW	Once in a lifetime – an event that will generate national headlines and considerable media attention	VERY LOW	(£100s)	No evident impact on performance / objectives. Readily recoverable, local, minor service disruption Negligible loss of resources. Minor inconvenience.	Single minor injury. Zero or minor injury or work absence.	Minor adverse publicity. No discernible impact on reputation. Isolated comment in media/ occasional complaint.

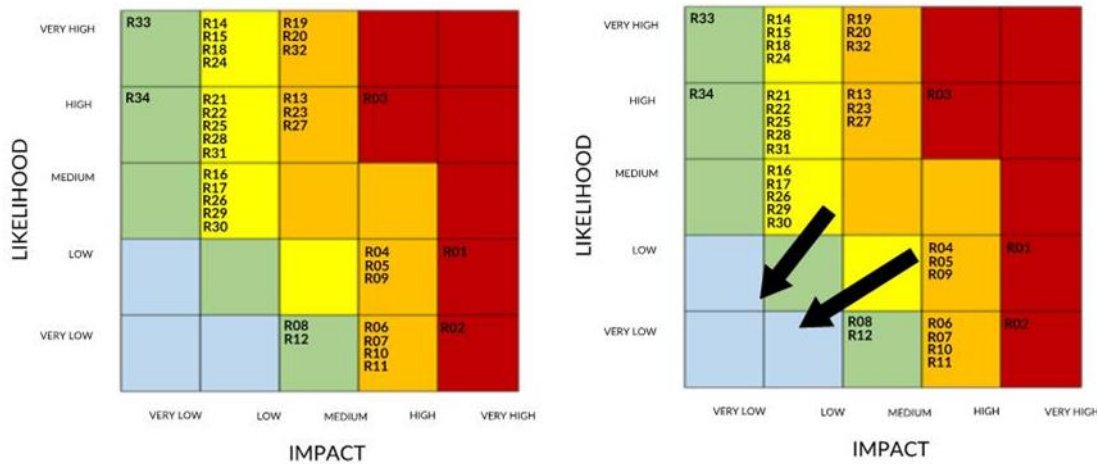


Appendix F - Develop security strategy

The intent of any risk treatment is to reduce the severity of those risks being treated. We refer to these as gross risk (pre-treatment) and net risk¹⁰ (post-treatment). This intent is also shown graphically in Figure 12. This net risk needs to be understood and accepted by the client – no risk treatment will eliminate risk completely, merely reduce it as low as is reasonably practicable (ALARP).

It has been assessed as appropriate for the project that those risks graded medium, high and very high are treated and that any lower risks will benefit from the aggregated risk treatments applied to other risks (i.e. they will also benefit from the identified treatments). These treatments are addressed in later sections of this strategy document.

Figure 12. Gross risk and net risk intent matrices



Source: Hoare Lea

Operational Requirements

Hoare Lea Security follow the “Operational Requirements” (ORs) approach set out by the UK’s Centre for Protection of National Infrastructure (CPNI). CPNI defines an OR as a statement of the overall security need. Combined, these form the security strategy. An effective security strategy not only mitigates the identified threats but also enhances efficiency of daily operations. In the context of a security strategy, the ORs represent the security recommendations as per BREEAM HEA06.

There are five main *effects* that should be considered in the development of the OR statements: DETER, DETECT, DELAY, RESPOND and RECOVER. Security requirements should demonstrate at least one of these intents. These are further defined below as.

- **DETER:** A measure that discourages a threat source’s target selection process.
- **DETECT:** A measure that identifies an attack from a threat source using real-time observation or post-incident analysis.
- **DELAY:** A measure that is intended to slow the progress of an attack.
- **RESPOND:** The action taken to address an incident to enable the assessment of any required actions.
- **RECOVER:** The restoration of an operational capability to a pre-incident state.

¹⁰ This is sometimes referred to as residual risk.

In the wider design environment, those ORs should also seek to support the following principles towards the creation of a safe and secure environment, whilst minimising the impact on the environment itself:

- Access and Connectivity** - Safe and secure places balance the need for access control with connectivity and circulation.
- Structure and Spatial Layout** - Safe and secure places are structured in a way that manages risk and conflict.
- Ownership** – Safe and secure places are those over which occupants and users have a sense of ownership and responsibility.
- Surveillance** - Safe and secure places have appropriate levels of both natural and technical surveillance.
- Activity** - Safe and secure places are active and welcoming to legitimate users.
- Physical Security** - Safe and secure places are appropriately and proportionately protected.
- Public Image** - Safe and secure places are well maintained, managed and promote a positive public image.
- Adaptability** - Safe and secure places are adaptable to change.

Operation Requirements (ORs) identification

ORs are a key stage in laying the ground work of an effective security design. During their development, it is vital to consider how they can be delivered through physical, electronic or operational measures, or a combination of those measure. This process also requires the behaviours of the people assets to be considered during the identification of appropriate risk treatments, not only to secure the building, but also to ensure the proposed solution is not subject to bypassing due to perceived obstruction.

The ORs for this project have been identified against the risks within the security risk register. These have been defined against the identified risks and can be seen in Table 11.

A summary of key recommendations and ORs can be seen in Table 3. These represent the security recommendations as per BREEAM HEA06. Within this table, indicative solutions and implications for the design team have been captured.

Phase specific strategies

Phase specific strategies have been developed based upon the site-wide operational requirements. These can be seen in the following appendices:

- Appendix G: Phase 1: Plots E and F
- Appendix H: Phase 2: 1 Station Hill Plaza, The Rest and surrounding podium levels.
- Appendix I: Phase 3: Plots A, B, C, D, Station Hill Gardens and the basement levels, including the parking.

For each phase we have carried out the following:

Security strategy development

The permissible access and circulation of different user groups is analysed alongside the development of the vulnerability relationship network diagrams. Once understood, this allows the subsequent security strategy to be analysed and developed through the establishment of security zones.

Security zoning

This is one of the key operational requirements that is identified in any built asset development and sets the baseline for security layering and the development of asset specific security measures during the next design

stage. It also allows for the identification of areas needing a more focussed security input and further development (to be undertaken in subsequent design stages).

Once layouts are frozen, this security zoning can also then be applied to these. The zonal strategy devised for the development can be seen below.

PUBLIC Accessible to everyone at all times with no ability to impose control measures	
SEMI PUBLIC Space that is easily accessible to the general public. Typically restricted outside of normal hours.	
SEMI-PRIVATE RESIDENTIAL Predominantly for the use of a limited, authorised population within residential spaces. Usually employs an electronic or procedural access control measure. Guests and visitors usually escorted.	
SEMI-PRIVATE COMMERCIAL Predominantly for the use of a limited, authorised population within commercial spaces. Usually employs an electronic or procedural access control measure. Guests and visitors usually escorted.	
SEMI-PRIVATE BOH Predominantly for the use of a limited, authorised population within BOH spaces. Usually employs an electronic or procedural access control measure. Guests and visitors usually escorted.	
SEMI-PRIVATE CO-WORKING Predominantly for the use of a limited, authorised population within commercial co-working spaces. Usually employs an electronic or procedural access control measure. Guests and visitors usually escorted.	
PRIVATE COMMERCIAL Private areas with limited access to authorised individuals (commercial employees). Guests usually escorted.	
PRIVATE RESIDENTIAL Private areas with limited access to authorised individuals (residential tenants). Guests usually escorted.	
PRIVATE LANDLORD BOH Private areas with limited access to authorised individuals (FM staff/BOH). Guests usually escorted.	
RESTRICTED Contain critical or sensitive assets and/or reserved for a very exclusive user group (i.e. security staff). Contractors may be allowed but would always be escorted.	

Appendix G – Phase 1 (Plots E & F)

Security strategy graphic

The security strategy graphic, 2525046-HL-02-ZZ-SM-Y-680-4010 summarises the security strategy detailed in the operational requirements derived within the security risk assessment.

Security strategy (zoning) drawings

The following zoning drawings have been produced to support design development.

Plot	Floor	Drawing number
E & F	Ground floor	2525046-HL-XX-00-DR-Y-680-0003
E & F	Level 1	2525046-HL-XX-01-DR-Y-680-0004
E & F	Level 2	2525046-HL-XX-02-DR-Y-680-0005
E & F	Level 3	2525046-HL-XX-03-DR-Y-680-0006
E & F	Level 4	2525046-HL-XX-04-DR-Y-680-0007
E & F	Level 5	2525046-HL-XX-05-DR-Y-680-0008
E & F	Level 6	2525046-HL-XX-06-DR-Y-680-0009
E & F	Level 7	2525046-HL-XX-07-DR-Y-680-0010
E & F	Level 8	2525046-HL-XX-08-DR-Y-680-0011
E & F	Level 9	2525046-HL-XX-09-DR-Y-680-0012
E & F	Level 10	2525046-HL-XX-10-DR-Y-680-0013
E & F	Level 11	2525046-HL-XX-11-DR-Y-680-0014
E & F	Level 12	2525046-HL-XX-12-DR-Y-680-0015
E	Level 13	2525046-HL-XX-13-DR-Y-680-0016
E	Basement 1	2525046-HL-XX-B1-DR-Y-680-0002
E	Basement 2	2525046-HL-XX-B2-DR-Y-680-0001

Appendix H – Phase 2 (1 Station Hill Plaza, The Rest and surrounding podium level)

Security strategy graphic

The security strategy graphics, 2525046-HL-02-ZZ-SM-Y-680-5020 and 2525046-HL-02-ZZ-SM-Y-680-5030 summarise the security strategy detailed in the operational requirements derived within the security risk assessment.

Security strategy (zoning) drawings

The following zoning drawings have been produced to support design development.

Plot	Floor	Drawing number
G	Podium level lower ground	25-25046-HL-02-P1-DR-Y-680-0003
G	Podium level – Lower ground Mezzanine	25-25046-HL-02-P2-DR-Y-680-0010
G	Ground Floor	25-25046-HL-02-GF-DR-Y-680-0020
G	Level 01	25-25046-HL-02-01-DR-Y-680-0030
G	Level 02	25-25046-HL-02-02-DR-Y-680-0040
G	Level 03-07	25-25046-HL-02-ZZ-DR-Y-680-0050
G	Level 08	25-25046-HL-02-08-DR-Y-680-0060
G	Level 09	25-25046-HL-02-09-DR-Y-680-0070
G	Level 10-14	25-25046-HL-02-ZZ-DR-Y-680-0080
G	Level 15	25-25046-HL-02-15-DR-Y-680-0090
G	Level 16	25-25046-HL-02-16-DR-Y-680-0100

Appendix I – Phase 3 (Plots A, B, C, D and the basement levels, including the parking)

Security strategy graphic

The security strategy graphics, 2525046-HL-03-ZZ-SM-Y-680-6020, 2525046-HL-03-ZZ-SM-Y-680-6030 and 2525046-HL-00-ZZ-SM-Y-680-7010 summarise the security strategy detailed in the operational requirements derived within the security risk assessment.

Security strategy (zoning) drawings

The following zoning drawings have been produced to support design development.

Plot	Floor	Drawing number
A,B,D	Basement 3	25-25046-HL-03-B3-DR-Y-680-0040
A,B,D	Basement 2	25-25046-HL-03-B2-DR-Y-680-0030
A,B,D	Basement 1	25-25046-HL-03-B1-DR-Y-680-0020
A,B,D	Ground floor	25-25046-HL-03-GF-DR-Y-680-0001
A,B,D	Level 01-05	25-25046-HL-03-ZZ-DR-Y-680-0010
C	Basement	25-25046-HL-2C-B1-DR-Y-680-0001
C	Ground floor	25-25046-HL-2C-GF-DR-Y-680-0010
C	Level 01	25-25046-HL-2C-01-DR-Y-680-0020
C	Level 02	25-25046-HL-2C-02-DR-Y-680-0030
C	Level 03-08	25-25046-HL-2C-ZZ-DR-Y-680-0040
C	Level 09-19	25-25046-HL-2C-ZZ-DR-Y-680-0050
C	Level 20-23	25-25046-HL-2C-ZZ-DR-Y-680-0060
C	Level 24	25-25046-HL-2C-24-DR-Y-680-0070



DAVID CROFT

PRINCIPAL SECURITY CONSULTANT

+44 20 3668 7229

davidcroft@hoarelealea.com

HOARELEA.COM

Western Transit Shed
12-13 Stable Street
London
N1C 4AB
England

