Building mounted signs

Before affixing a street lamp or traffic sign to a building, the authority will have to serve notice in writing on the building's owner no less than 56 days before the date on which they intend to commence the works. For further information please refer to the Code of Practice for Affixing Traffic Signs and Street Lighting to Buildings in London (2015) for exercising the powers set out in section 45 of the Public Health Act 1961 and section 74 of the Road Traffic Regulation Act 1984 as amended by clause 4 of the London Local Authorities and Transport for London (No. 2) Bill.

Low level signage

- Design teams should consider how to minimise the visual and physical intrusion of low level signage such as traffic bollards
- Integrating pedestrian and cycle signage within bollards can be an effective way of reducing the need for larger post mounted signs
- 'Keep left' signs should be provided only where a road safety audit has identified the need

Figure 247: Integrated bollard mounted cycle signage



Location

Placement standards	
Horizontal clearance width between sign assembly and the carriageway kerb edge	
Absolute minimum for roads subject to a 30mph speed limit or lower	450mm*
Absolute minimum for roads subject to a 40mph speed limit or more	650mm
Absolute minimum for flush surfaces (no kerb upstand)	800mm
Vertical sign clearance height above pedestrian only footways	
Absolute minimum	2,100mm*
Preferred minimum**	2,400mm

** Please refer to LCDS for guidance on sign placement next to cycle tracks*
***Clearance heights may be increased to discourage vandalism*

Repeater signs on posts should be mounted at uniform height across a given length of road.

Sign design

Sign dimensions

Design teams should refer to the Traffic Signs Manual and TSRGD to select the current size of regulatory or warning sign appropriate for the traffic speed. Refer to Appendix A of the Local Transport Note 1/94: Design and Use of Directional Informatory Signs for further information on directional sign heights and siting distances.

Illumination

Signs should not generally be illuminated unless legally required to, as specified in TSRGD.

Fonts

The smallest text size appropriate for the traffic speed should be used, to keep overall sign sizes to a minimum.

Figure 248: Signage content should be clear and legible for users



Content

Design teams should consider how signage can be simplified to include only essential information and optimise legibility, subject to any strategic or local signing requirements.

Finish

The finish of sign posts and the sign reverse should coordinate with lighting columns and similar street furniture within a given locality. The use of grey or yellow 'backing boards' behind signs should be avoided unless considered absolutely vital to road safety.

Legislation, statutory powers and consents

On the TLRN, only TfL has the statutory power to permit traffic signs to be erected or removed.

Figure 249: TLRN traffic restriction



All signs installed on the TLRN must comply fully with the standards outlined in the TSRGD. Expert advice should always be sought from a specialist to ensure compliance.

Statutory requirements and detailed guidance on the design of signing for the public highway are provided in the TSRGD. For sign legends not covered in TSRGD, separate special sign authorisation is required from the DfT. The proposals put forward in the DfT's policy paper, Signing the Way, give greater local flexibility and discretion in the design of non-standard signing and provide a framework for the removal of traffic signals. Further guidance is given in the TSM and the Local Transport Note (LTN) 1/94.

Signs requiring legal backing by road traffic orders can take up to three months to process and adequate time must be allowed in programmes to accommodate this.

Additional information

Legislation:

Traffic Signs Regulations and General Directions (TSRGD)

Department for Transport:

Traffic Advisory Leaflet 01/13 (2013): Reducing Sign Clutter

Signing the Way 2011: Traffic Signs Policy Paper

Traffic Signs Manual 1982 and 2013

Local Transport Note 1/94: Design and Use of Directional Informatory Signs

12.2. Bollards and low level traffic signs

Bollards tend to be overused or inappropriately located which can create clutter and pose a hazard for those with visual impairments. Bollards are used to discourage vehicles from encroaching on to pedestrian or cycle space, preventing vehicles from running over hidden basements, preventing damage to footway surfaces, street furniture and buildings while reducing the risk of pedestrian injury.

Bollards should be treated as a last resort solution and should only be used when all other alternatives have been exhausted. Other necessary street furniture or equipment should be reviewed to identify if it could be used instead to perform the same role as a bollard. Enhanced enforcement may also be a preferable solution to bollards to deter vehicles from encroaching on the footway.

Please consult the local authority conservation team when considering the removal or reuse of historic bollards.

Figure 250: Bollards protecting footway space



Alternatives

Design teams should consider where appropriate:

- Using street furniture or equipment to create a barrier using cycle racks, tree planting, seating, etc
- Using containment kerbs or high edge kerb upstands (140mm or more)
- Local strengthening of the footway where vehicles are known to mount the kerb

Layout considerations

For instances where it has not been possible to provide alternatives to bollards:

- Bollards should be arranged to minimise physical clutter while maintaining an appropriate defensive line; this may not necessarily be a straight line but could involve setting back bollards to align with other street furniture such as tree planting
- Filtered permeability, whereby motor vehicles are blocked but cycle access remains, can be achieved through the appropriate placement of bollards or street furniture across the carriageway
- Bollards are not required at side road entry treatments as they create additional clutter and do not provide protection for pedestrians

Safety

- Formal risk assessments may be required for the provision or retention of bollards
- Design teams should question any pre-existing arrangement of bollards and consider removal subject to safety advice

Bollard placement standards	
Minimum distance from kerb face	450mm
Recommended distance between bollards to prevent vehicle access	1,200mm (except for 'keep left' bollards)
Recommended distance between bollards for stopping vehicles from mounting the footway	At 3,000mm centres across width of footway
Bollard design standards	
Minimum bollard height	1000mm (except for keep left bollards)
Visibility bands	150mm band of contrasting colour

**Please note that these standards do not apply to security bollards which have their own defined manufacturer's specification and placement requirements*

Types of bollard

Bollards are available in a wide range of materials; where possible we have a general preference for bollards made with polymers that pass Head Injury Impact and Chest Impact tests.

Bollard designs should be selected based on the function they need to fulfil:

- The design should be appropriate for the character of the area
- Removal bollards may be appropriate for areas which are largely pedestrianised to restrict general vehicle access but allow for servicing vehicles
- A number of traditional historic bollards exist on the TLRN, some of which are listed, and should be retained
- The method of ground fixing should be detailed to minimise damage to the surrounding footway, should a vehicle collision occur, allowing for easy replacement of the bollard
- Bollards should not be linked with chain or rope

Options	General on footway	Removable posts	Security bollards
Image			
Application	Preferred design for urban areas	Where a street requires temporary vehicular access for servicing or maintenance	Station and building security
Dimensions	1,000mm height ±100mm Tapered Round	Minimum 1,000mm height	Must be specified and fixed in accordance with Publicly Available Specifications (PAS) 68 and 69 Round domed top
Colour	RAL coated black RAL signal grey	RAL coated black RAL signal grey	Silver grey
Material/finish	Flexible polymer	Flexible polymer	Stainless steel
Lighting	Unlit with white visibility bands	Unlit with white visibility bands	Unlit with visibility bands

Traffic bollards

Bollards can also be used as a mount for displaying traffic signs, but there is no legal requirement for a bollard to have a sign. Those which have a sign are classed as 'traffic bollards' and provide low level traffic signage through the use of permitted directional and pedestrian/cycle signs.

Low level signs permitted for use on bollards, DfT, TAL 03/13: Traffic bollards and low level traffic signs.

Options	'Keep left' – hoop bollard	Bollards with additional signage	Bollards with additional signage
Image			
Application	Preferred design for central urban areas and town centres	Preferred design for urban areas	Rural, suburban and conservation areas only
Dimensions	800mm height ±200mm 400mm width ±100mm	1,000mm height ±100mm Tapered Round	Recommended 1,000mm height Square diamond top
Colour	RAL coated black RAL signal grey	RAL coated black RAL signal grey	
Material/finish	Flexible polymer	Flexible polymer	FSC accredited wood
Lighting	Unlit	Unlit	Unlit with etched visibility bands

Figure 251: Signage types. Traffic signs are Crown copyright



'Keep left' bollards

There is no highway authority requirement to provide a 'keep left' bollard (TSRGD diagram 610) on a traffic island. Designers should assess whether a traffic bollard is required on a site-by-site basis.

Self-righting retroreflective 'keep left' bollards should be used as an alternative to illuminated bollards on the TLRN to improve safety and reduce maintenance.

Retroreflective coating, or coloured panels, should not be used on the rear face of bollards.

The luminance requirements for traffic bollards are set out in BS EN 12899-2:2007.

Additional information

Department for Transport:

Traffic Advisory Leaflet 03/13: Traffic bollards and low level traffic signs

Legislation:

Traffic Signs Regulations and General Directions (TSRGD)

Equality Act 2010

British Standards:

Publicly Available Specifications (PAS) 68 and 69

BS EN 12899-2:2007 Fixed, vertical road traffic signs. Transilluminated traffic bollards (TTB)

12.3. Street nameplates

The effective design and installation of street nameplates is essential for assisting the general public in navigating the road network, while also ensuring more efficient functioning of postal and emergency services.

This guidance is directed at local authorities to ensure a high standard of application for a feature that is present on almost every street in London.

Placement

Street nameplates should be positioned as near to street corners as possible to be easily read by all street users. Recommended placements should consider the context of the street and the relationship of adjoining streets.

Street nameplates should be mounted on to walls, buildings or other boundaries at the back edge of the footway where practical. Nameplates at major junctions should be positioned so as to receive illumination from adjacent street lights.

Post-mounted nameplates should only be used in exceptional circumstances where the sign would otherwise be obscured.

Figure 252: A street name plate



Acceptable mounting height	600-3,600mm
Preferred height	1,000mm
Preferred height where low level obstructions are likely	2,500mm
Major crossroads	Fixed at each street corner
Minor crossroads	One plate on each side of the street adjacent to the emerging traffic
T-junctions	Main street nameplate positioned directly opposite side road
Change in street name on same street	Sign both street names with arrows if desired
Long stretches without an intersection	Repeater signs at reasonable intervals and opposite entrances to places such as rail stations

Design

Street nameplates are commonly viewed from an acute angle and so the size and choice of font and spacing should be as legible as possible. Lettering is recommended to be at a height of between 75mm and 90mm. The minimum spacing between words should be approximately 50 per cent of the height of the lettering. Top and bottom borders should be approximately 40 per cent of the lettering height.

Street nameplates should provide strong visual contrast between the lettering and the sign background. The most effective colour contrast is black lettering on a white background. The preferred material for the plate is box-formed vitreous enamel.

Figure 253: Street name plates should provide strong visual contrast between lettering and the background



Most local authorities have a particular style of nameplate that they adopt for the majority of streets in their area. In many boroughs a coloured postcode and borough name has been introduced to provide additional information. The postal area and direction of house numbers may also be included to assist navigation. If district names are to be included on the street nameplate, reduced lettering heights should be used.

Where historic signage contributes to local character these should be retained and refurbished wherever possible.

Authorisation and maintenance

Local authorities are responsible for the installation and maintenance of street nameplates. Any proposal to move or erect street nameplates, should involve the relevant local authority.

It is recommended that the London boroughs regularly monitor the quality of street nameplates and building numbering in their area to ensure they are of a good standard, prioritising street nameplates at junctions.

Renaming

Any proposal to rename a street as part of a major streetscape improvement project requires authorisation by the local authority. Where approved, the old name should be crossed out and remain clearly legible below the new name. It should be retained for one to two years, before being considered for removal. Street nameplates with historic interest should be preserved wherever possible.

Additional information

Legislation

The Local Government (Miscellaneous Provisions) (Northern Ireland) Order 1995. No. 759 (N.I. 5). Part 11: Street names and numbering of buildings

Sections 64 and 65 of the Towns Improvement Clauses Act 1847 (TICA)

Sections 17-19 of the Public Health Act 1925 (PHA)

Local Government Act 2003

Joint Mobility Unit:

Sign Design Guide, 2000

London Transport Users Committee:

Where am I? Street name signs in London, 2003

12.4. Barrier free footways

Pedestrian guardrails

Pedestrian guardrails are known to give the impression of vehicle dominance, clutter, reduce kerbside activity, increase maintenance and block major pedestrian desire lines.

We have a presumption against the use of pedestrian guardrails in new schemes and will investigate removal where safe to do so.

The Local Transport Note LTN 2/09 – Pedestrian Guardrailing (PGR) notes that, 'there is no conclusive evidence that the inclusion of PGR at any type of pedestrian crossing or junction has any statistically significant effect on the safety record'.

Designers are encouraged to look at our Guidance on the Assessment of Pedestrian Guardrail for additional advice.

Figure 254: Guardrailing often restricts free movement by non motorised users



Guardrail removal

Streetscape Guidance promotes the removal of existing guardrails where a proven safety requirement cannot be demonstrated. Road safety audits should be undertaken in any guardrail removal assessment to determine the safety implications.

Partial removal of guardrails may be recommended to alleviate pedestrian pinch points. Guardrails on side roads adjacent to the TLRN may be located within the borough boundary, and so approval with the borough should be sought when requesting removal.

A cycle parking audit should be undertaken before removal to ascertain if the guardrail is used for cycle parking. Sufficient replacement cycle parking stands should be included accordingly as part of the removal process.

Monitoring

Periodic reviews should be undertaken to record any problems with guardrail removal, especially relating to collision numbers. This should be entered into the Traffic Accident Diary System (TADS) for long-term collision monitoring.

Guardrail retention

- The reinstatement of existing guardrails requires SDRG approval. Guardrails may be retained where a road safety audit confirms that pedestrian desire lines put pedestrians at risk, or on signalised pedestrian crossings. Please refer to the Guidance on the Assessment of Pedestrian Guardrail for additional advice.

Figure 255: Junction of Lancaster Place and the Strand before and after guardrail removal





New provision of guardrail

We will not support the installation of new guardrails except where a road safety audit has demonstrated a clear need. SDRG approval must be sought for any new pedestrian guardrails. Any new guardrails must be black.

Additional information

Transport for London:
Guidance on the Assessment of Pedestrian Guardrail, 2012

Department for Transport:
Local Transport Note (LTN 2/09): Pedestrian Guardrailing, 2009

12.5. Barriers

Vehicle restraint systems in the form of safety fences and barriers are installed on major arterial routes where vehicles travel at high speeds to contain vehicles on-carriageway and prevent collisions with oncoming traffic or roadside hazards.

Safety should always be the primary factor in deciding whether to install restraint barriers; however, the design, scale and build of the barrier should also be carefully considered to minimise the detrimental visual impact this kind of infrastructure can have on the overall streetscape.

Location

Designers should be conscious of streetscape considerations relating to the character of the road network and how road restraint systems create a visual and physical barrier between either side of the street.

Designers should acknowledge pedestrian desire lines and aim to reduce unnecessary severance caused by barriers by implementing alternative means to complete their journey.

Figure 256: Barrier provision is essential on certain roads across the network



Figure 257: The correct placement of barriers within the streetscape should be carefully considered



Design

Many types of safety fences and barriers are available to provide containment of vehicles. These include tensioned and untensioned corrugated beams, open box beams and concrete safety barriers; concrete providing the most robust treatment. A safety expert should always be consulted to select an appropriate product and detail the placement to best meet the requirements for the road environment and the hazard.

Safety fences and barriers are usually galvanised and should not be finished in black.

Where a safety barrier is provided in a busy pedestrian setting, designers are encouraged to provide a treatment on the reverse face which conceals fixings and has a smooth textured finish.

The placement of safety fences on grassed verges on higher speed roads should take account of the need to cut vegetation around the fence supports. It may be appropriate to incorporate a hard surfaced strip to remove the need to cut around the fence supports.

Where equipment is located behind a barrier, adequate vehicle access must be provided to give a position behind the barrier to allow safe operation of a mobile elevating work platform (MEWP). Alternatively, consideration must be given to changing a fixed CCTV column to a trolley head column where only a car size vehicle is required for maintenance.

Assessment process

A Road Restraint Risk Assessment process should be conducted on all trunk roads with speeds of 50mph or more, as detailed in DMRB Volume 2, Section 2, Part 8: Requirement for Road Restraint Systems. The assessment is also required on trunk roads with lower speed limits, where a potential roadside hazard has been identified.

The assessment process provides a framework to support designers in making the optimal site specific design decision on restraint requirements, while using a robust safety methodology.

Additional information

Department for Transport, Highways Agency:

Design Manual for Roads and Bridges: Volume 2, Section 2, Part 4, TD19/85: Safety Fences and Barriers

Design Manual for Roads and Bridges: Volume 2, Section 2, Part 8, TD19/06: Requirement for Road Restraint Systems

Manual of Contract Documents for Highway Works, Volume 1, Series 400: Road Restraint Systems (Vehicle and Pedestrian)

Manual for Streets (2007)

British Standards:

BS 7669-3: Guide to the installation, inspection and repair of safety fences

12.6. Utility cabinets

Utility cabinets (including signal controller cabinets) are generally located above ground to minimise installation costs and provide convenient access for maintenance.

We recognise the necessity for utility companies to have safe and efficient access to services; however, the proliferation of utility equipment within the street environment increases the visual impact on the streetscape and, if unchecked, can create additional unnecessary obstructions on the footway. Therefore, utility cabinets should be kept to a minimum.

Figure 258: Utility boxes placed at the back of the footway



Location

When utility companies seek to introduce a new cabinet on the road network, clear footway width must satisfy footway clear zones as described in Streetscape Guidance.

Cabinets should preferably be located at the back of the footway, away from windows or walls where they could assist in unlawful entry into properties. Cabinets must not physically or visually obstruct loading bays, service access points or crossovers. Exceptionally, if a utility cabinet is to be installed adjacent to the kerb, it must be positioned within the furniture zone.

Where a utility cabinet is to be located within a planted or grassed area, a minimum 500mm wide hard surface must be provided around the cabinet to allow for adequate access and to facilitate the maintenance of shrubs and grass.

Where a cabinet cannot be located against the back of the footway, doors should open so that utility operatives face towards the carriageway or oncoming traffic

Design

- Utility companies should be encouraged to use cabinets of a consistent and simple design
- The colour of the utility cabinet should be a black finish throughout London. Consideration may be given to the provision of non-standard finishes, such as green or beige, where there is an alternative palette of surrounding street furniture or if the utility cabinet is situated next to a listed building or structure
- Low-profile clear matt anti-graffiti finishes should be applied to facilitate the removal of graffiti and flyposters
- In exceptional circumstances and upon approval from both the utility company and the SDRG, bespoke covers or finishes can be provided to reduce the visual impact of the utility cabinet

12.7. Feeder pillars

Electrical feeder pillars are cabinets located within the highway boundary, designed to manage and distribute power to local electrical assets such as traffic equipment.

Always consult an electrical engineer when locating and specifying a feeder pillar unit. For instance, where the nearest supply source is not readily accessible it may be necessary to install additional isolating pillars.

Location

Pillars should be located at the back of the footway, adjacent to a wall or fence, where the likelihood of damage from vehicular collision is reduced, but away from locations where they could assist in unlawful entry into properties. They should be positioned to avoid creating a trip hazard, obstructing private property, doorways, accesses, shop windows or footways. All pillars should be oriented so that the door is easily accessible for a maintenance engineer.

The distance from a feeder pillar to the equipment it serves should generally not exceed 20 metres, due to electrical and fusing requirements. More than 20 metres can be used, but needs careful consideration by a suitably qualified electrical engineer.

Figure 259: Pillars should be placed away from pedestrian desire lines



Feeder pillars within grass verges should have a hard standing paved surround to enable convenient access.

Design

- Designers are encouraged to use cabinets which minimise the visual and physical intrusion of the feeder pillar in the street
- The size and type of pillar should be selected based on its functional requirements: small pillars for where a site supply is not metered, large pillars where it is metered, and generator connect pillars where supported by an external generator
- The colour of the feeder pillar should be a black finish throughout London. Consideration may be given to the provision of non-standard finishes, such as green or beige, where there is an alternative palette of surrounding street furniture or if the utility cabinet is situated next to a listed building or structure
- All hinges and locks should match the colour and finish of the main unit
- Pillar doors must be fitted with standard keys to allow distribution network operator (DNO) and maintenance engineer access
- Where equipment is fixed to a shared column and systems contain low voltage circuitry, for electrical safety reasons this will require the power for all equipment to be supplied from the same source, with each having a separate isolator
- A large feeder pillar may have to be used to accommodate the extra equipment

Additional information

British Standards:

BS 7671: Requirements for Electrical Installations

12.8. Variable message signs

Variable message signs (VMS) are designed to provide greater flexibility than standard road signs to inform users of changing network conditions. The display of temporary information can be used to alter customer behaviour, assist in improving traffic flow and network operation, alerting customers to:

- Congestion conditions along a corridor
- Construction and maintenance schedules
- Special event notifications
- Weather warnings
- Incident notifications

The variable messaging system is controlled remotely and enables the sign to show mandatory and/or advisory information depending on local, real-time requirements.

VMS are now being installed as permanent structures across major arterial routes and high roads. They may also be installed on a temporary basis during roadworks or planned events.

The installation of these signs can positively influence behaviour and may assist them to achieve quicker and safer journeys.

Figure 260: Variable message sign (VMS) when not in use



They are particularly effective for roads which provide an important strategic function on the network, helping to maintain good network performance by offering useful information.

Location

VMS are generally large units which can significantly impact on the visual character of the streetscape. Design teams should consider the scale of the signage relative to other streetscape elements and identify whether the network performance benefits of integrating a VMS into the street are outweighed by the impact on quality of place. When locating signs in conservation areas please consult with the local authority conservation officer.

VMS are costly to install and should be prioritised where issues of safety have been identified on the network. In conservation areas the use of VMS should be limited. On arterial motorway routes, with road speeds of 40mph or more, two VMS signs displaying the same legend should be implemented where possible.

The location should be selected based on site specific data collection requirements regarding safety, traffic speeds, existing signage, road capacity and the location of utilities. VMS units can be attached to existing structures.

Design of unit

- The material and finish of signposts should coordinate with other street furniture
- The sign face should be black when a message is not being displayed
- Controller cabinets should be located within 30 metres of the VMS display and should be black, positioned at the back of the footway or adjacent to the VMS
- Cantilevered signs are preferred to two post footway mounted signs on high roads, to minimise the number of poles used
- Gantry signs are large, overhead structures that should only be considered on high capacity arterial roads. The overhead position is more readily visible and legible for high speed roads; however, the large size of the structure is only appropriate for wide carriageway dominant settings
- Consideration should be given to combining VMS with electronic advertising boards with reference to statutory limitations on the use of VMS signs for this purpose
- Footway mounted sign heights should be increased to 3000mm where signs are adjacent to cycle or equestrian routes

The design of the unit and the mounting position determines the separation standards for placement of VMS on the network:

Mount	Height	Context
Overhead gantry sign	Minimum 5,500mm from carriageway surface	Arterial routes only
Cantilevered sign	Minimum 2,400mm from footway surface, 600mm from the kerb edge to any point on the sign	Arterial, high roads, city hubs
Verge sign/footway mounted	Minimum 2,400mm from footway surface	Arterial, high roads, city hubs

VMS placement standards	
Minimum distance between two verge mounted signs	200 metres
Minimum distance between two gantry mounted signs	300 metres

Types of display

Three types of display may be considered for use on the TLRN, with certain pros and cons for each medium. It is possible on larger signs to combine technologies within the same sign. Designers should select the display type based on how the sign is anticipated to be used, the type of information to be displayed, and if a wide range of information is required with symbols:

- Electro-mechanical – rotating planks with two or three faces or prisms can be used to give additional versatility to a standard fixed-faced traffic sign
- Reflective flip-disk – matrix of disks, one side black, the other fluorescent, flipped magnetically by electrical current. These signs are well suited to showing combinations of letters or symbols as a message
- Light-emitting – fibre optic or light-emitting diode technologies. The major advantage of these signs is that a greater range of messages can be displayed than for reflective technology signs

Sign design considerations

Sign designers need to consider a number of factors including:

- Sign sizes
- Character height
- Legibility
- Contrast and viewing angle
- Ambient illumination levels and expected approach speeds

Messaging

- Messages, symbols and abbreviations used on VMS shall conform to Regulation 58 and Schedule 15 of the TSRGD
- Standard messaging shall be from the Transport alphabet typeface prescribed in Regulation 13 and illustrated in Schedule 13 of the TSRGD
- Signs should never contain more than 10 words nor provide conflicting messages on any one sign
- When VMS are used as warning signs, it is usual for them to be fitted with four amber-flashing lanterns, subject to the provisions of Regulation 58
- Where a second sign is provided on a central reservation, it should only ever duplicate the message displayed on the verge sign

Authorisation

The appearance and legend of VMS signs should conform to Regulation 58 and Schedule 15 of the TSRGD. Sign designs and formats not conforming to the TSRGD are required to be authorised by the Secretary of State.

Applications for authorisation should in the first instance be addressed to the relevant government regional office or Highways England for trunk roads in England.

Additional information

Legislation:
Traffic Signs Regulations and General Directions (TSRGD) (Regulation 58)

Department for Transport, Highways Agency:
Design Manual for Roads and Bridges (DMRB), Volume 8, Section 2, Part 2 TD 33/05 The Use of Variable Message Signs on All-Purpose and Motorway Trunk Roads

12.9. Environmental monitoring equipment

Monitoring of local environmental conditions is important for quantifying the quality of the environment across the network. TfL and other authorities capture air quality and other environmental data to help inform policy and drive environmental improvements.

While environmental monitoring equipment may be necessary, it is vital that the placement and design of the equipment does not detract from the quality of the streetscape, safety or functionality.

Location

The position and size of the monitoring equipment will generally be determined by data collection requirements. Roadside monitoring is most common for emissions analysis; however, there are many considerations in locating environmental equipment within the street environment. From a strategic perspective, analysers must be suitably distributed to capture the data required for the study. They should not be located at point sources of high pollution unless that is a particular aspect to the study.

Smaller equipment should be mounted on existing columns and can be powered by batteries. Larger units will require a direct power supply, which may be able to be drawn from a nearby facility without extensive ducting. A broadband line may also be required to monitor data capture remotely.

The physical and visual impact of the unit should be considered such that any larger units avoid obstructing footways and sightlines. Special consideration should be given to the location of the equipment if it is required within a conservation area.

Units do not necessarily need to be located directly next to the carriageway and so may be installed at the back of footway, within building recesses or integrated with another facility. Site operators should be able to access all parts of the unit.

Designers should acknowledge the impact that the duration of study will have on siting the monitoring equipment. In certain situations, indicative monitoring may be sufficient over a few months, but in other cases more detailed monitoring will be required for a year or more.

Design

- A range of analyser types are available to capture data for different kinds of particulates and pollution
- To minimise the impact on the streetscape, a simple, clean, modern design of housing unit is preferred, matching the colour of adjacent street furniture
- Anti-graffiti and flyposting finishes should be applied, as used for control boxes and other utility cabinets
- The equipment being used determines the size and type of housing unit
- In most situations, monitoring equipment would benefit from being in an enclosed temperature controlled unit. This will however increase costs and the size of the unit required
- It may be useful to install meteorological sensors to capture local conditions and complement other datasets
- Planning consent may be required by the local authority for larger monitoring units

Additional information

Department for Environment Food & Rural Affairs:
Local Air Quality Management: Technical Guidance, 2009

Figure 261: Discrete monitoring equipment



12.10. Roadside cameras and CCTV

Introduction

Cameras are used by TfL and other authorities for several purposes:

- To enforce traffic regulations such as speed limits
- To enforce bus lane restrictions
- To enforce the central London Congestion Charge scheme
- To provide information on traffic congestion
- To assist the police with enforcement duties
- To monitor journey time

We share some cameras with London local authorities to reduce proliferation by promoting sharing and multitask equipment. When installing or replacing cameras a priority should be given to renewing or creating partnerships between suppliers to work towards reducing clutter.

Placement

The type and location of cameras is almost entirely governed by the function they are required to perform and the area of view they are required to cover. All cameras impact on the streetscape when mounted on columns. Wherever possible, cameras should be combined with lamp columns or attached to adjacent buildings or structures to reduce clutter, however, expert advice must be sought from an engineer prior to undertaking the work.

Prior to installing a camera on a building, the owner must first give consent and planning and listed building consent must also be sought if necessary. Installing a camera on a building may also require associated legal costs, annual rentals, maintenance agreements and bespoke mounting devices.

When mounting CCTV cameras on existing lamp columns it is vital to ensure that columns are capable of accommodating the additional load and are sufficiently rigid to minimise camera shake.

Where new lamp columns are being installed, consideration should be given to combining lighting with CCTV and roadside cameras. This will require a more rigid column (240mm diameter standard) than is typically installed for lamp columns and mechanical separation of the electrical supply. Designers should also consider the impact of light flare from the adjacent lighting unit

Where CCTV and roadside cameras are located on columns, the control equipment should be located separately in a cabinet on the footway, in accordance with the guidance on traffic signal control cabinets. Camera columns should be aligned in the furniture zone, especially in urban areas.

Figure 262: Enforcement cameras



A standard column height is eight metres, but poles also come in six, 10, 12 and 17 metre heights, however, safety cameras have their own requirements – please speak to our Traffic Infrastructure team for further information.

Design criteria

While some CCTV cameras may be attached to buildings or structures, many are located on high masts. CCTV cameras should be mounted on the most slender poles possible but must not be subject to camera shake.

When placed on grass areas there must be adequate hard stand around the column and a hard access route across the grass area, this must also be provided for the cabinet and power supply.

Roadside cameras require an electrical supply and a clear, unimpeded view of the highway. Safety cameras also require associated carriageway markings to support information recorded by the camera.

Fixed safety camera housings must be coloured yellow either by fully painting the front and back of the housing, or fully covering both with retro-reflective sheeting. The location of low level roadside cameras for speed, traffic signal or bus lane enforcement also needs to be conspicuous to avoid any claims of entrapment.

Materials

The function that the camera must perform often dictates the type of camera chosen

- **Shoebox camera** – allows for high optical zoom therefore best used when monitoring from greater distances. Shoebox cameras are commonly used for enforcement duties and perform better in low light conditions. They tend to be more expensive than a dome camera
- **Dome camera** – uses digital zoom therefore best used when monitoring areas of shorter distances. It is commonly used for monitoring traffic conditions and is less expensive than a shoebox camera
- **Automatic number plate recognition (ANPR) camera** – used to capture detailed shots of licence plates and the vehicles that have committed traffic violations. Also used to measure average vehicle speeds over several points
- **Safety camera** – used to capture traffic violations



Dome camera



Shoebox camera



Automatic number plate recognition (ANPR) camera



Safety camera

There are several types of column that can be used to mount a camera. The location, maintenance requirement and the speed and volume of traffic will influence the type of column used. Please contact our Traffic Infrastructure team for further information.

Fixed column

- Cheaper installation costs but more expensive to access and maintain
- Carriageway may need to be closed to access and service the camera
- Can be combined with other street equipment more readily therefore reducing clutter

Wind down trolley head

- Eliminates the use of mechanical lifts for servicing thereby reducing maintenance costs
- Area required to service the camera is reduced

Mounted on buildings

- Visual impact is reduced
- Require the permission of the building owner to access
- Require a maintenance agreement with the building owner
- Installation and operation costs can be more expensive

Figure 263: Mounting options



Fixed pole



Wind down trolley head pole



Combined with lights



Mounted on buildings

Data collection

Most street improvement projects will require some degree of on-street data collection, which may include pedestrian flow counts and classified vehicle counts. While some of this process can be conducted manually, more extensive data collection will require the temporary installation of cameras to capture movement data.

Cameras should be fixed securely to existing columns and should not obstruct the footway or impair roadside operational requirements. Contractors should ensure that any fixtures will not damage the adjacent street furniture. The temporary equipment and the mounting stands should match the colour of the surrounding street furniture.

Figure 264: Data collection cameras



Authorisation

Legislation:

Section 63 of the Road Traffic Regulation Act 1984 as amended by the Transport Act 2000 (Section 75)

Additional information

British Standards:

BS 7671 Requirements for Electrical Installations

12.11. Planned events infrastructure

Designing in permanent infrastructure to support planned events may be considered in exceptional circumstances for the delivery of certain key services on roads which regularly serve as a focus for significant citywide events. This may include reinforcing designated areas of footway for planned HGV overrun or for locations where generators will be accommodated during events.

As a general principle, streets should be designed for flexible use so that they can serve as focal points for activity when required.

In all cases we have a duty to 'assert and protect the rights of the public to the use and enjoyment of any highway for which they are the highway authority' (Section 130 of the Highways Act 1980) and so any temporary or permanent infrastructure to support a planned event should uphold this bond.

Other permanent event infrastructure

Design teams may wish to include additional services such as power sockets and fixtures to assist in the hosting of major events. Post mounted banner arms may be considered for lamp columns on roads which serve as major event routes.

Any other non-standard permanent item of street furniture should be approved by the SDRG. Bespoke features should be integrated with the streetscape palette to minimise the visual impact.

Additional information

Legislation:
The Highways Act 1980

Licence application:
http://www.tfl.gov.uk/info-for/urban-planning-and-construction/

Transport for London:
Highway Licensing and Other Consents, 2011
Network Operating Strategy, 2011

Figure 265: Some of London's streets regularly serve as a focus for major events



Part E Street environment

13.1 Street environment 275
13.2 Growing a greener London 275
13.3 Keeping London dry 285
13.4 Lighting the way 295
13.5 Leftover spaces 305
13.6 Pocket parks 309



13.1 Street environment

London's street environment is influenced by a range of features which contribute significantly to the creation of distinctive and successful places. These features shape the look and feel of our streets, and vary between more obvious streetscape items, such as lighting columns and trees which should be positive attributes of the streetscene, to largely unnoticed or hidden structures such as drainage systems which are critical in the operation and management of it.

The importance of these features cannot be understated as they often 'set the scene' for life to take place on a street. They can also improve the experience of the street by providing tangible benefits such as pleasant, green social spaces for the enjoyment of local communities, and by improving surface runoff and water quality through an integrated sustainable urban drainage system (SuDS) network; to more intangible benefits such as enhancing the perception of safety in an area during the evening.

Figure 266: Trees can reinforce movement patterns and also provide a comfortable place to wait for the next bus



13.2 Growing a greener London

Vision

Much of the green infrastructure (GI) in London – including street trees, woodland, planted areas, grass and wildflowers – can be found alongside the road network. It is hugely important that these assets are properly planned, maintained and managed by the relevant arboriculture and landscape professionals. Delivering a cleaner, greener streetscape is central to achieving the

Figure 267: All public realm schemes should contribute to increasing the amount of green infrastructure across London



strategic goal of tackling climate change and enhancing the built environment.

Our vision is to ensure that the greening of our streets is an integral part of scheme development, optimising the potential of our streets for contributing to the GI agenda. There are a wide range of benefits associated with GI including improving air quality and human health, surface water runoff, mitigation of the urban heat island effect, increased biodiversity and ecosystem variety, and amenity value through creating beautiful and visually interesting streets and spaces for people to enjoy. All schemes within London – ranging from footway renewal to the wholesale redesign of a street – should ensure that all opportunities for improving and introducing new GI elements are fully explored.

Trees

New tree planting should be considered wherever appropriate within schemes. Working with trees means that designers are using a living organism that will grow, change and develop over time, it is therefore vital that the relevant arboricultural specialist is engaged at all stages of a scheme involving proposed trees.

Location

It is important that a range of considerations are taken into account when determining the location of a new tree. In some instances, trees have been planted in locations inappropriate for the development or lifetime maintenance of the tree, or without considering alterations to its immediate surroundings over time. Factors to consider when locating new trees include (but are not limited to):

- Street signs and traffic lights
- Proximity to dropped kerbs
- Footway width
- Proximity to carriageway

Figure 268: Working with trees requires taking into account the growth, development and maintenance of the tree over its lifetime



- Designated parking bays
- Proximity to other existing GI
- CCTV splays and equipment
- Proximity of buildings
- Heritage features
- Risk of subsidence
- Underground/overhead utilities
- Advertising hoardings
- Accessibility for future maintenance

Where possible, trees should be located within the furniture zone so as to provide the maximum footway clear zone for pedestrian movement (refer to 'Footway zones' in this guidance for further information). As with many street furniture items, the placement of trees should also help to reinforce public realm design elements such as:

- Strengthening movement patterns and corridors
- Connecting spaces and providing visual continuity across them
- Aiding the reinforcement of space and boundaries
- Providing character and a sense of place
- Enhancing architectural elements
- Screening to vehicle corridors and undesirable views

Figure 269: It is important that careful consideration is given to providing the optimum location for trees within the public realm



Species considerations

Once a suitable location has been identified, the relevant highway authority arboricultural specialist must be engaged to determine the appropriate tree species and specification to be used. The tree species planted should take account of existing trees and the long-term aspirations for the area, and should give due consideration to:

- Ultimate height, crown spread, stem diameter and habit
- Honeydew from aphids
- Fruit fall
- Ability to cope with a changing climate
- Pests and diseases
- Maintenance requirements
- Water requirements
- Scale of setting; Wildlife and Countryside Act 1981 Schedule 9
- Climate change adaptation benefits, including shade

Tree pits and surface specification

There are many different tree pit specifications of varying complexity, but no one design will be suitable in all situations and options should be agreed with the highway authority's arboricultural and landscape officer. Elements of the tree pit which must be considered include:

- Pit dimensions
- Soil specification
- Anchoring method
- Edging material
- Use of root cells/root barriers

While organic bark mulch is typically used as a surface material around newly-planted trees in hard landscapes, there are a range of surface materials which can be used depending on individual circumstances.

It must be remembered that newly-planted trees require an appropriate programme of irrigation to establish and thrive. This might involve hand watering or an automatic system; the relevant arboricultural and landscape specialist must be

Figure 270: A range of tree pit and surface materials are available and should be chosen based upon the location and specific requirements of the tree







								
Selection criteria	Gravel: Resin bound	Gravel: Self binding	Grilles	Mulch: Inorganic	Mulch: Organic	Rubber crumb	Soil	Asphalt
Tree criteria								
Permeability for air and water to reach the rooting medium if correctly maintained	**High**	**Medium**	**High**	**High**	**High**	**High**	**High**	**Low**
Flexibility of material	**Medium**	**High**	**Low**	**High**	**High**	**High**	**High**	**Medium**
Risk of damaging young tree health if incorrectly installed	**High**	**High**	**Medium**	**Low**	**Low**	**Medium**	**Low**	**High**
Risk of damaging established tree health if incorrectly installed	**Low**	**Low**	**High**	**Low**	**Low**	**Low**	**Low**	**Medium**
Risk of damaging young/established tree health if unmaintained	**Medium**	**Low**	**High**	**Low**	**Low**	**Medium**	**Low**	**Medium**
Potential to improve soil fertility	**Low**	**Low**	**Low**	**Low**	**High**	**Low**	**Medium**	**Low**
Suitability for installation up to the base of a young tree	**Low**	**Medium**	**Low**	**High**	**High**	**Medium**	**High**	**Low**
Site criteria								
Tolerance to regular pedestrian traffic	**High**	**Medium**	**High**	**Low**	**Low**	**High**	**Low**	**High**
Resistance to street sweeping machines/animal excavation	**High**	**Low**	**High**	**Low**	**Low**	**High**	**Low**	**High**
Effectiveness at suppressing weed growth	**Medium**	**Medium**	**Low**	**High**	**Medium**	**Medium**	**Low**	**High**
Availability of different colours/styles	**High**	**Low**	**High**	**High**	**Low**	**High**	**Low**	**Medium**
Installation and maintenance criteria								
Suitability for installation immediately after tree planting	**Medium**	**Medium**	**High**	**High**	**High**	**Low**	**High**	**Low**
Likelihood of requiring a subbase prior to installation	**High**	**Low**	**High**	**Low**	**Low**	**High**	**Low**	**High**
Level of experience/competence required to correctly install and maintain	**High**	**Medium**	**High**	**Low**	**Low**	**High**	**Low**	**Medium**
Expected lifespan of material	**Medium**	**Medium**	**High**	**Low**	**Low**	**Medium**	**Low**	**High**
Whole life cost of material, including purchase, installation, maintenance and disposal	**High**	**Medium**	**Medium**	**Low**	**Low**	**High**	**Low**	**Low**

engaged to determine what system/specification is most appropriate. Further guidance concerning irrigation can be found in the London Tree Officers Association (LTOA) guidance document Sustainable Water Management: Trees are part of the solution.

For existing trees, a range of surface materials can be used including (but not limited to):

- Gravel: Resin bound
- Gravel: Self binding
- Mulch: Inorganic
- Mulch: Organic
- Rubber crumb

Each surface material has its advantages and disadvantages and no one surface treatment is suitable for all situations. Guidance for material selection can be found in the LTOA document 'Surface materials around trees in hard landscapes'. The table (below) from the LTOA document should be read in conjunction with it.

If planting trees directly into the ground is not possible then it might be appropriate to use raised planters. Many different designs of planter are available and the relevant arboricultural and landscape specialist must be consulted in the selection of the appropriate product. It should be remembered that using planters could have implications on tree health, may attract litter/vandalism, require a higher degree of maintenance and will constitute an increased irrigation burden.

Maintenance

Trees differ from other assets in that they often appreciate with age and have less predictable life spans and maintenance regimes than built assets. They must be adequately protected when worked around in accordance with the principles set out in the documents National Joint Utilities Group Guidelines 4 (NJUG4) and British Standard 5837 – Trees in relation to design, demolition and construction.

In cases where tree roots are conflicting with footway materials the relevant arboricultural specialist must be consulted to find a suitable solution. This may involve extending the tree pit or manipulating or pruning the roots, although the latter is only to be undertaken on instruction from the relevant arboricultural specialist.

Removal of any item of green infrastructure is to be considered only when all other

Figure 271: Mature trees on Victoria Embankment



practicable solutions are not viable. If removal is considered necessary, this must only be undertaken with the consent of the arboricultural and landscape officer and may require planning permission, permits and licences, or senior management approval.

Lights in trees

The installation of lights in trees can be problematic and is generally not encouraged. However, if unavoidable then a suitable design must be developed which does not damage the tree. The relevant arboricultural and electrical specialists must be involved in this process.

Lights may require regular removal to inspect or maintain the tree. When installing lights in trees consideration must also be given to the location and installation of any feeder pillars. These must not have a detrimental impact on either the tree and in particular the root system, or pedestrian movement through the area.

Figure 272: Tree lighting should be carefully considered with relevant arboricultural specialists



Trees on the TLRN

Trees on the TLRN are the responsibility of TfL's arboriculture and landscape maintenance managers (A&LMM), who work in accordance with our Green Estate Management Plan (GEMP).

We require a minimum three-year guarantee on all new trees planted on the TLRN. Advice on planting of new trees, irrigation and maintenance must be sought from the A&LMM.

Tree removal on the TLRN is taken very seriously and is subject to a robust tree removal procedure. The removal of healthy trees is generally considered a last resort and should only be considered when appropriate to do so.

All trees on the TLRN are inspected on an annual basis for defects with work undertaken as necessary in accordance with the GEMP and best industry practice. Data pertaining to trees on the TLRN is held on the Network Asset Management System (NAMS) database.

All street trees on the TLRN have been assigned a monetary value using the Capital Asset Value for Amenity Trees (CAVAT) system as hosted by the LTOA. TfL will seek to secure compensation based on the CAVAT valuation for any damage which is caused to our trees.

Planted areas

Planted areas include woodland, shrub beds and hedges which can comprise a variety of deciduous and evergreen, native and non-native species. Each is managed according to function, species mix, age, condition and location. Species choice is vital to the success of any planting scheme and must take account of site factors and management requirements, including the following aspects:

- Function, for example screening
- Maintenance (access and frequency of operations)
- Tolerance to pests and diseases
- Tolerance to drought
- Tolerance to pollution and the ability to trap particulate matter
- Tolerance to road salt
- Tolerance to light or shade
- Life expectancy
- Seasonal interest (flower, fruit, foliage, stem colour)
- Biodiversity and wildlife objectives
- Ultimate natural size of plants
- Habit/form
- Antisocial considerations, as advised by the community safety officer

The ability to cope with a changing climate is also essential for all new planting schemes. Fixed irrigation systems are generally not sustainable due to ongoing maintenance and costs, and often cannot be used during hosepipe bans.

Green infrastructure may provide a sustainable urban drainage system function where surface water is dispersed through the soil rather than discharged into the highway drainage system. The replacement of hard surfaced areas with new grassed or planted areas can also contribute to SuDS, landscape integration, enhancing the built environment and visual amenity, nature conservation and biodiversity, and providing areas to support larger trees. Where new grassed or planted areas are proposed over old hard surfaces, such as footway or carriageways, it is essential to break out the old roadbed. Unless specifically designed as a SuDS measure, planted and grassed areas should not be relied upon as the main measure for the discharge of surface water.

Planted and grassed areas must be designed with consideration of existing and proposed pedestrian desire lines. Shrubs with thorns and spikes can act as a deterrent but must not be relied upon as the main measure to stop inappropriate access and can collect litter.

Planted areas should be designed with careful consideration of the realities of urban life and avoid the creation of concealed places close to pedestrian areas. Raised planted areas close to seating can become hotspots for needle disposal and litter accumulation. Raised planted areas are also discouraged in new schemes as they may require more regular watering over the lifetime of the planting scheme.

Occasionally, some areas of herbaceous and bedding plants or special horticultural features will require special maintenance operations. Hanging baskets are permitted, subject to appropriate licence approval.

Grassed areas

Grassed areas comprise highway verges, embankment and cutting slopes, central reserves and traffic islands. Some grassed areas have significant biodiversity interest and habitat value, supporting protected species of flora and fauna.

Any works on or around grassed areas must be in accordance with industry best practice. If it is necessary to track over a grassed area for construction or maintenance purposes, protection is required to limit the impact of heavy equipment to the satisfaction of the highway authority's arboriculture and landscape officer. Full reinstatement will be required to make good any damage.

Reinforced grass (plastic or concrete) measures may be used, following approval by the highway authority's arboricultural and landscape officer, to aid in reinforcement of grassed verges where residential off-road parking or access to properties is permitted.

The following are essential design considerations for newly grassed areas:

- Achieve the intended maintenance regime and required permits
- Avoid placing street furniture in grassed areas as additional trimming will be required
- Maintain sightlines, visibility and access where low frequency and wildflower grass verges are proposed
- Planting of seeds or plants of local provenance where existing habitats and wildflower areas might be compromised by the introduction of non-local species
- Should be of sufficient width to allow effective maintenance and avoid edges and corners becoming easily degraded
- Ensure that grassed areas are located away from strong pedestrian desire lines to avoid the grass becoming downtrodden
- Choose more drought tolerant grass species to limit irrigation regimes

Grassed areas on the TLRN

There are three broad grass maintenance regimes used on the TLRN:

A. Regular cut grassed areas with a high, medium or low frequency depending on the location. High frequency areas are high profile spaces and include 'town streets' and 'city places'. A medium frequency maintenance regime is usually more appropriate for verges in locations characterised by slower speed and higher residential populations such as 'local streets' and 'high roads', while a low maintenance regime is appropriate for higher speed road verges and central reserves on 'connectors' and 'arterial roads'.

B. Grassed areas with bulbs add seasonal interest and local colour. They are maintained as regular cut grass with the exception that the areas containing bulbs remain uncut for six weeks after flowering to allow energy reserves to return to the bulb underground. During this period the verge can appear unmanaged, but regular cuts to adjacent verges indicate that maintenance is active.

C. Wildflower (species-rich) grasslands have historically been limited to high-speed arterial roads but improved establishment and maintenance techniques have led to an increase in popularity and use in higher profile urban areas. They can add long periods of flowering and create habitat for insects, but the lower maintenance regime leads to longer grass which can appear unsightly if not carefully designed for succession flowering. Wildflowers grow best on nutrient-poor soils where competition from weeds is reduced. Understanding the soil conditions before sowing wildflowers is essential as weed control on fertile soils can be very difficult and expensive.

Figure 273: Planted areas form a large part of London's green infrastructure



Wildflower areas require one or two visits per year which reduces the need for permits and the emissions from cutting machinery. Litter collection, usually by the local authority, is a more difficult task in longer grass but is essential to ensure that the site is safe and litter-free before grass cutting.

Our A&LMMs are responsible for the management of all aspects of the Green Estate including planted areas in accordance with the GEMP. They must be consulted and approve all works and proposals which may affect it.

Passeig de St Joan Boulevard Barcelona, Spain

Creating a vibrant urban green zone using permeable paving and tree planting

Key functions

Opportunity

A wide, hazardous and unsightly footway in Barcelona has been transformed into a sustainable and vibrant green zone that better uses the available space.

Benefits

Through unobtrusive intervention this development has revitalised the social value of the boulevard, catalysing commercial and recreational use of the area while improving biodiversity.

Implementation

The poor condition of the Passeig de St Joan Boulevard was becoming a hazard for pedestrians. Instead of resurfacing the footway, an ambitious remodelling was undertaken. Space was allocated between pedestrian, recreational and cycle use. This was achieved by reducing the space allocated to traffic and by segregating the cycle lanes. Two new rows of trees were planted to improve the aesthetic quality of the boulevard. Adequate drainage into subsoil was an issue; this was facilitated through the use of a permeable pavement system which added to the appeal and sustainability of the site.



Images courtesy of Adrià Goula

Applying in London

Where wide footways allow, shared space can be created for pedestrians, cyclists and those wishing to stop and sit.

Chelsea Fringe London, UK

Making the most of existing infrastructure

Key functions

Opportunity
The Chelsea Fringe is an open source and largely free festival that runs for about three weeks every year from mid May to early June.

Benefits
The open access principle of the fringe ensures that almost anything goes from temporary to permanent installations, community-led garden initiatives, exhibitions, events, experiences, exhibits and talks and walks across London.

Implementation
The Chelsea Fringe, although independent from the RHS Chelsea Flower Show, runs with its support. The fringe is largely volunteer run and hosts a wide range of events. These are generally free and centred on plants and gardens.

Applying in London
With such a broad scope of potential events, the Chelsea Fringe has the ability to reach more Londoners than many other events. TfL has provided a platform for some Chelsea Fringe events that are sponsored by a third party or the applicant. All future events are subject to approvals from asset owners and the SDRG.

Additional Information

British Standards:
BS 5837:2012 Trees in relation to design, demolition and construction – Recommendations (BSI)

BS 4428: Code of practice for general landscape operations

Forestry Commission
Right Trees for a Changing Climate: (www.righttrees4cc.org.uk)

Greater London Authority:
Greenspace Information for Greater London (GiGL) (www.gigl.gov.uk)

Highways Agency (HA):
Design Manual for Roads and Bridges (DMRB): Volume 10, Environmental Design and Management, HA, Section 3: Landscape Management

DMRB: Volume 10, Environmental Design and Management, HA, Section 0, Part 2: Environmental Functions

DMRB: Volume 10, Environmental Design and Management, HA, Section 0, Part 3: Landscape Elements

London Tree Officers Association (http://www.ltoa.org.uk/):
Surface materials around trees in hard landscapes

Sustainable Water Management: Trees are part of the solution

National Joint Utilities Group:
NJUG Guidelines for the Planning, Installation and Maintenance of Utility Apparatus in Proximity to Trees, 2007

Susdrain (http://www.susdrain.org/)

Transport for London:
Green Estate Management Plan

Trees and Design Action Group:
Trees in Hard Landscapes: A Guide for Delivery, 2014

UK Roads Liaison Group:
Well-maintained Highways, 2013

New York City Department of Transportation:
Street Design Manual

13.3 Keeping London dry

Intense rainfall puts London at risk of localised flooding from surface water running off ever increasing impermeable surfaces. Effective rainwater management is vital to the functioning and enjoyment of London's road network.

With greater focus on the need to manage surface water runoff, we encourage designers to consider water-sensitive design principles and to explore opportunities for incorporating sustainable urban drainage systems as an approach to managing rainfall. For highway runoff, we will consider SuDS measures designed in accordance with the SuDS Manual (CIRIA C697) on a site-by-site basis.

Overview

London's drainage system is a complex interconnected arrangement of private and public drains and sewers, with public ownership in the hands of multiple highway and drainage authorities. Much of London's drainage assets are out of sight, hidden deep beneath our streets, but are nevertheless critical to keeping Londoners' feet dry. If these assets are poorly designed or not maintained in optimum condition, the effects can be devastating to local communities, disruptive to traffic flow and damaging to other highway assets.

Highway drainage systems must be designed to ensure minimal maintenance and a long life in terms of hydraulic and structural requirements. In addition, designers need to account for the potential impacts of extreme weather events, take steps to assess the risk of flooding, and take every opportunity to increase resilience.

The remainder of this section will focus on surface water drainage at the local level.

Types of drainage systems

There are many types of drainage systems available to manage rainwater. The size, shape, gradient and geology of a catchment area are all factors which can influence the type of system and materials used. London's highway drainage systems include:

- Attenuation tanks
- Balancing ponds
- Drainage pipes
- Filter drains
- Grassed surface water channels
- Kerbs and gullies
- Oil and petrol interceptors
- Soakaways
- Surface flow wetlands
- Surface water channels

Figure 274: A typical highway drainage system. There are features visible on the surface, such as covers and gratings as well as those buried and out of sight such as pipes and chambers



Typically drainage systems on the road network will consist of kerbs, channels, road gullies, and drainage pipes. The profile of the road surface forms an important function of this type of drainage system by guiding water towards gullies, minimising aquaplaning and splashing and maximising the longevity of the pavement and its associated earthworks.

Layout

Within the highway there are multiple elements which may influence layout and material choices. These include available outfalls for new systems, surface profile and steepness of gradients, pedestrian desire lines, constraints resulting from the location of utility services, the likelihood and impact of systems becoming blocked by detritus, trees and street furniture. All of these elements have knock-on effects to drainage systems above and below ground, so will influence the drainage design. For example, road gullies should be sited to intercept surface water immediately before a pedestrian crossing point and drainage pipe runs should avoid tree root systems.

Drainage systems need to have a minimal physical impact on the carriageway or footway. A well-designed and maintained road drainage system ensures:

- Safe conditions in all weather
- Minimal nuisance to pedestrians via splashing
- Minimal environmental impact
- Durability and robustness of the carriageway surface
- Minimal disruptions caused during regular maintenance

Where possible, drainage and possibly utility apparatus should be laid in 'corridors' in the footpath. This will improve ride quality and facilitate the future maintenance of the services with minimum impact on road closures. Refer to the NJUG Guidelines on the Positioning and Colour Coding of Underground Utilities' Apparatus (2007) for further information.

Cyclic maintenance activities are generally carried out without road space permits, hence thought needs to be given to positioning of gullies based on access and traffic flows.

Design criteria

The following is an overview of the requirements for typical drainage systems on the highway:

- New or upgraded drainage relating to highways shall be designed in accordance with the Design Manual for Roads and Bridges, the Specification for Highway Works, and Sewers for Adoption
- The principle adopted for all highway drainage should be the use of straight sections of pipe serving trapped gully pots. Pumping of surface water should be avoided
- Where it is not possible to install a gully pot due to depth of construction, a catch pit connected to a gully is permissible
- Designers should avoid the practice of connecting gully to gully as a means of transferring flows. Each gully pot should ideally have its own connection to the carrier pipe
- In exceptional circumstances short lengths of highway rider sewer will be allowed
- Preference should be given to flexible jointed pipes
- All access chambers shall be designed and constructed in accordance with Sewers for Adoption 7
- Gully pots shall be constructed in accordance with the appropriate standard detail and be of high performance concrete

- Gully covers shall be hinged, not lift out
- Cyclic maintenance activities are generally carried out without road space permits, hence thought needs to be given to positioning of gullies based on access and traffic flows

Trees and drainage systems

Trees, like drainage, are an essential element of any good street. Care must be taken when working with planting and drainage infrastructure to ensure that one does not affect the other causing increased maintenance requirements.

Tree roots are attracted to moisture leaving drainage infrastructure through defects, cracks and displaced joints. Slow flowing drainage and standing water at the surface may indicate a blockage due to root infiltration. If the defects are not detected and addressed by routine maintenance the roots will continue to grow, expand and exert pressure at the crack or joint where they entered the pipe. The force exerted by the root growth will over time break the pipe and may result in its total collapse, attracting a higher cost to bring the asset back to an acceptable level of service. Therefore all new drainage systems near existing or newly planted trees must be designed to prevent root infiltration.

Topography of carriageway profiles

The size and shape of a drainage area, as well as the length and gradient of the surface have an effect on the surface water runoff. CCTV surveys may be required to confirm whether existing drainage facilities are underperforming and whether new drainage facilities are required. Topographic surveys will need to be provided along with a localised gully catchment plan for any required remedial works as well as to support the positioning of new drainage assets.

The combination of topographic surveys and local gully catchment plans can be modelled to show how effective the spacing of features such as gullies and carriageway profiles are and used to develop improved layouts to reduce ponding and aquaplaning.

This analysis can be refined when looking at specific locations such a crossing points, turning circles and bus stops where there is a higher potential of ponding and nuisance.

Cambers and falls

Gradients at building frontages should prevent surface water from entering buildings, basements or station entrances. Surface water should be intercepted before bus stops, pedestrian crossings and junctions. Falls should be encouraged to direct surface water into gullies as collection points. Please refer to HD39/01 Footway Design of the DMRB for further information on the design of crossfalls and longitudinal gradient.

Low point should be at the gully and not located at the crossing otherwise localised ponding will occur at the crossing. If the road cannot be profiled to create a gully low point additional/alternative drainage arrangements will have to be made.

Materials and maintenance

Regular maintenance can have a positive impact on the life of assets. For example, well-maintained road drainage will reduce the risk of water-logged foundation layers resulting in improved ability to withstand loading and minimise reactive repairs or premature failures.

It may be false economy to choose materials on cost alone as there may be high maintenance costs if proprietary products or special maintenance activity is necessary to maintain an asset. Key to an excellent drainage system is ensuring that the need for disruptive traffic management during maintenance is kept to a minimum. Therefore it can be cost effective to invest in high performance materials at the outset.

Installation of ironworks and covers needs appropriate consideration and material specification. The following items need to be considered when installing a cover:

- Potential loading and strength of materials
- Manual handling limitations
- Noise generation
- Friction
- Seating
- Differential settlement
- Milling when resurfacing is carried out

The use of traditional covers and their associated construction methods have resulted in a history of failure without any warning, often resulting in lane closures at peak times and significant disruption to journey times. Taking appropriate consideration at design stage reduces the potential for high cost reactive defects and the risk of potential third party claims for compensation.

Grates

A gully grate is a slotted cover to a gully pot. Grates prevent objects from washing into gullies, thereby reducing the risk of blockages and flooding. Designers need to select the correct grating type and positioning of gullies. It is not good practice to position gully gratings adjacent to crossing points where they are a potential trip hazard.

Cycle friendly grates: In any location where there is a possibility that cycle wheels will cross gullies, the grate slots should be at right angles to the direction of travel. Alternatively, non-slot 'pedestrian style' gratings should be provided.

Pedestrian friendly grates: In any location where there is a high likelihood that a pedestrian will walk directly across the gully, this form of grate should be provided. These grates should be slip resistant and also prevent narrow heels from getting trapped. The grate should be at right angles to the direction of travel.

High volume grating: These may be used on the network where cycles are not permitted. High volume grates are at risk of capturing cycle wheels in the grating due to the large gaps required to capture higher rates of rainwater.

Slot channels: Consideration should be given to the maintenance implications of slot channels which can block with debris unless routinely cleared.

Channels: In some instances designers may need to install channels in the footway. Dished channels should be avoided as they do not provide a level walking surface. Due consideration should be given to their positioning and surrounding surfaces.

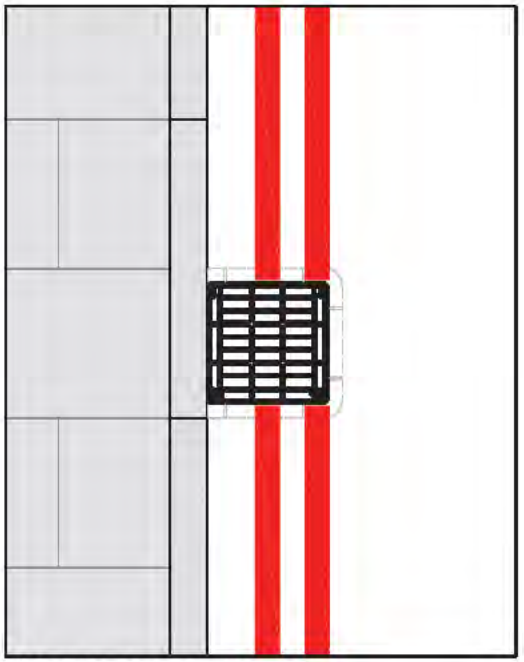
Figure 275: Cycle friendly grate on TLRN



Figure 276: Channel and pedestrian friendly gully

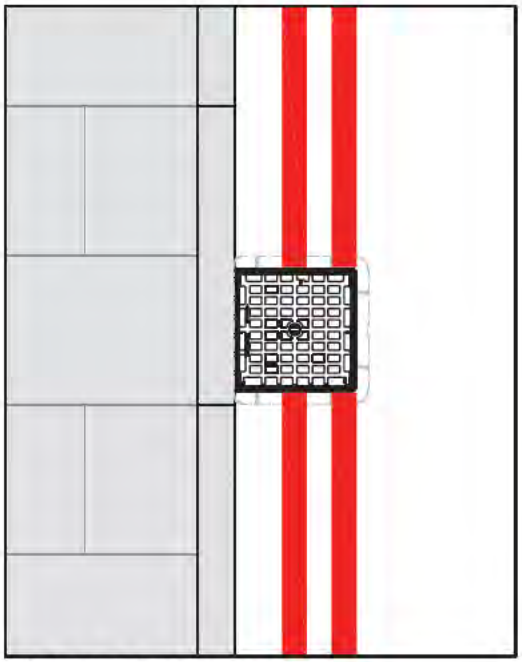


Figure 277: Carriageway gully grate types



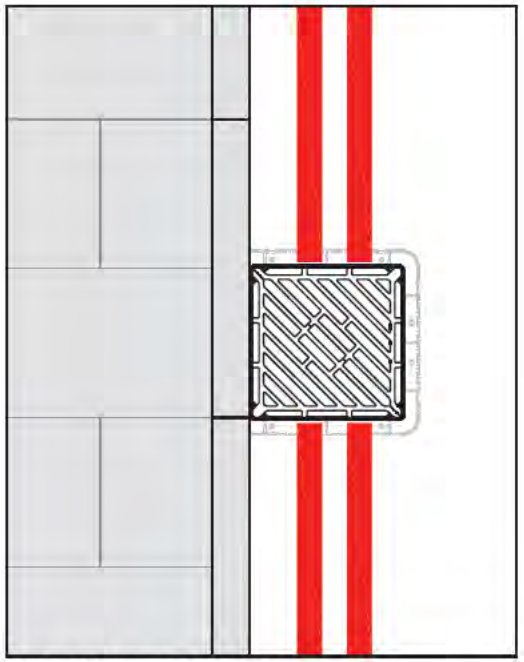
CYCLE FRIENDLY GRATE

Grate slots should be at right angles to the direction of travel.



CYCLE FRIENDLY GRATE

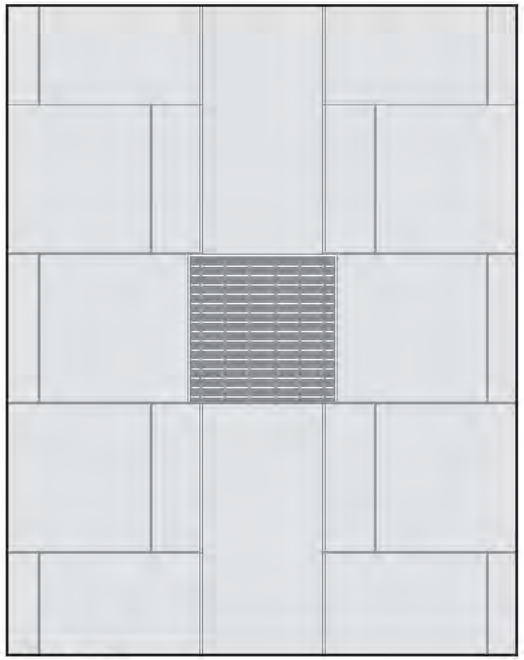
Cycle friendly grates can take several forms, this being another example. These grates should be slip resistant. While they are also pedestrian friendly they should not be in a pedestrian crossing.



HIGH VOLUME GRATES

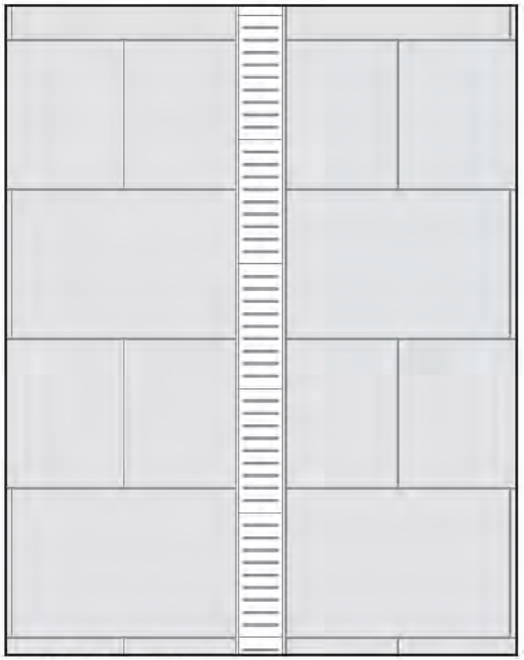
Above is an example of a high volume grating that may be used on the network where cycles are not permitted.

Figure 278: Footway drainage options on footway



CHANNEL

This is an example of a pedestrian friendly gate. Spaces between slots in footway grates should be between a minimum of 6mm and a maximum of 10mm to avoid heels becoming trapped.



LINEAR CHANNEL

Consideration should be given to the maintenance implications of linear channels which can block with debris unless routinely cleared.

Sustainable urban drainage systems and attenuation systems

Sustainable urban drainage systems manage surface water caused by rainfall. Approaches to managing rainfall can address water quantity (flood mitigation) as well as its quality (pollution reduction). SuDS may also provide amenity value when incorporated with green infrastructure.

Sustainable drainage is normally achieved by managing rainwater close to where it falls, by providing areas where rainwater can be stored – normally within natural contours – so that it is allowed to soak (infiltrate) into the ground, evaporate into the atmosphere or be used by vegetation (evapotranspiration) or be released slowly back into the conventional (piped) drainage system.

Designers should not propose options that:

- Cause a negative net effect to the Green Estate
- Do not consider whole life costs
- Are not technically feasible

With the greater focus on the need to reduce surface water runoff, we encourage designers to apply water-sensitive urban design principles so that green infrastructure is not lost, especially to impermeable surfaces, and to explore opportunities for incorporating SuDS measures to hold surface water and to manage its release into the piped drainage system. Where SuDS incorporate plantings, please consult an arboriculture and landscape manager.

Figure 279: Braham Street Park, Aldgate, uses a granular surfacing



Figure 280: Derbyshire Street, Bethnal Green, directs water into planted beds by using gaps in the edging



(Image courtesy of Greysmith Associates)

Permeable and porous surfacing

Porous and permeable surfaces allow rainwater through the surface layer to dissipate into underlying permeable soils. London is underlaid with a foundation of clay, which is ostensibly impermeable. However, there are locations throughout London where the soils are permeable and are able to remove rainfall from the surface. Whether or not the site in question has permeable soils, permeable and porous pavements may offer attenuation solutions which drain into a conventional (piped) system. Permeable and porous surfaces are becoming more readily available commercially. With appropriate consideration these could be incorporated into water collection features.

Proposals should be brought to the SDRG at the initial design stages.

Rain gardens and SuDS

Rainfall can be collected and directed from the footway or carriageway into a planting bed or tree pit, provided the tree is a suitable species. This can be achieved through the use of swales, permeable surfaces, kerb extension planters, street planters, and tree pits. Where space is available and is technically feasible these options should be considered. Please speak to an aboricultural and landscape maintenance manager for species selection when working on the TLRN.

Green walls

Vertical green walls using rainwater runoff from roof systems can play an important part in improving the streetscape. However, there is a high cost associated with the installation and maintenance of green walls. Therefore careful consideration is required at early design stages to whole life costs. All green wall proposals need SDRG approval.

Figure 281: Edgware Road green wall



The Stockholm Solution Stockholm, Sweden

Creating healthier street trees through water attenuation

Key functions

Opportunity

Trees in Stockholm, Sweden, have been used as part of a cost-effective system to manage excessive stormwater runoff.

Benefits

Stormwater tree trench systems reduce the reliance on existing drainage systems, improve safety by removing water ponding from footways and carriageways, and reduce splashing from passing vehicles.

Implementation

The trees are connected by an underground infiltration structure. Under the paving, a trench is created and lined with permeable fabric and filled with stone or gravel. Stormwater runoff flows through a special inlet (storm drain) leading to the stormwater tree trench. The runoff is stored in the empty spaces between the stones, watering the trees and slowly infiltrating through the bottom. If the capacity of this system is exceeded, stormwater runoff can bypass it entirely and flow into an existing street inlet.



Image courtesy of Wolf Paving Company, Inc.

Applying in London

Stormwater tree trenches should be considered in areas that are prone to flooding. This type of infrastructure should be investigated in Opportunity Areas and areas of regeneration.

Porous pavement trial London, UK

Water attenuation for safer streets

Key functions

Opportunity

Porous pavements offer highway authorities and developers a new tool to manage stormwater by allowing it to drain through the pavement surface into a stone recharge bed and infiltrate into the soils below.

Benefits

Porous materials remove excess water from carriageways and footways, improving driving conditions in wet weather and reducing splashing from moving vehicles.

Implementation

Porous pavements work by providing the water with a place to go, usually in the form of an underlying, open-graded stone bed. As the water drains through the porous asphalt and into the stone bed, it slowly infiltrates into the soil or to an attenuation system. The stone bed size and depth must be designed so that the water level never rises into the asphalt. This stone bed, often 450mm to 900mm in depth, provides a tremendous subbase for the asphalt paving.



Image courtesy of Wolf Paving Company, Inc.

Applying in London

Porous pavements are being trialled on the TLRN to determine if their use is appropriate and under what circumstances. We will publish results when the trial is complete.

Attenuation and infiltration systems London, UK

Replicating natural systems to provide easily maintained, aesthetically pleasing drainage capacity

Key functions

Opportunity

New and existing developments disrupt natural drainage of rainfall. While conventional drainage systems reduce flood risk, there are other smaller landscape features that can briefly attenuate or infiltrate rainfall and add visual amenity and ecosystem benefits.

Benefits

Attenuation and infiltration systems can reduce flood risk while also improving the ecology and visual amenity of the site.

Implementation

Following consultation with urban designers and ecologists, the raised kerbs installed in Potters Fields Park, London Bridge, were designed with slots between them to direct water off the kerb and footway into the adjacent gardens. This infiltrates a small amount of the flow and provides the gardens with a plentiful water supply.



Applying in London

Successful attenuation and infiltration systems require early consultation with several professionals to ensure structural, operational and maintenance issues are considered. These systems work well in areas of high footfall and where an opportunity to beautify the landscape exists.

Additional information

British Standards:

BS EN 124: Gully tops and manhole tops for vehicular and pedestrian areas

BS 8301: Drainage

BS 7903: Guide to selection and use of gully tops and manhole covers for installation within the highway

Department for Transport:

Design Manual for Roads and Bridges: Volume 4 – Geotechnics and Drainage

Department for Environment Food & Rural Affairs:

National Standards for sustainable drainage systems, 2011

National Joint Utilities Group:

NJUG Guidelines on the Positioning and Colour Coding of Underground Utilities' Apparatus, 2007

Construction Industry Research and Information Association (CIRIA):

The SuDS Manual (C697)

WRc Group (Water Research Centre):

Sewers for Adoption (7th edition), 2013

13.4 Lighting the way

Vision and purpose

To enhance night-time use, economy and enjoyment, and to provide safe passage across the Capital for all road users, we choose to provide street lighting across the TLRN. Street lighting provides many benefits to the network, including:

- Reducing night-time accidents and personal injuries
- Reducing crime and fear of crime

Figure 282: Highway lighting column illuminating footway and carriageway



Figure 283: LED lighting recently installed



(Image courtesy of CU Phosco Lighting)

- Promoting personal physical fitness and sustainability by encouraging walking and cycling after dark
- Facilitating social inclusion by permitting the use of streets and amenities after dark
- Supporting the 24-hour leisure economy promoting economic development
- Providing safe access to educational facilities supporting lifelong learning
- Assisting emergency services to identify locations and so reduce response times
- Permitting the effective use of CCTV during the hours of darkness
- Maintaining and/or improving the quality of life and personal wellbeing
- Providing an aesthetically pleasing appearance during the day and night

However, such advantages need to be considered with other benefits. These include their environmental impact, sustainability, the reduction in greenhouse gas emissions, the more efficient use of energy, and the provision of Best Value. Such initiatives are supported by drivers including the Climate Change Act 2008 (to reduce greenhouse gas emissions), the Carbon Reduction Commitment (CRC) Energy Efficiency Scheme (to make more efficient use of energy), and the Mayor's Transport Strategy and Climate Change Mitigation and Energy Strategy. We therefore embrace innovation and the latest technological advances to provide these outcomes and these include the implementation of a lighting Central Management System (CMS) and use of the latest light source technology.

Street lighting central management system

The current British Standard for road lighting recognises that road use often changes throughout the hours of darkness and with modern technology lighting levels on the carriageway can be adapted to meet those various requirements without compromising safety. We have therefore introduced a street lighting central management system to control and monitor each lighting point. This flexible approach to lighting and energy use supports the aforementioned aspirations.

This flexibility needs to be applied with London borough lighting policies in mind to ensure a consistent approach to road lighting across all of London's roads. Any proposed lighting installation on the TLRN will need to be CMS compatible.

Latest light source technology

For many years high intensity discharge (HID) lighting has been the mainstay of UK road lighting but advances in technology mean that the capability of solid state lighting now offers more energy efficiencies. We have trialled and are now installing LED technology across our road network. However, we are not committed to the use of only one technology since we aspire to the Institution of Lighting Professionals' (ILPs') mantra: 'the right light, in the right place, at the right time, controlled by the right system'. Where appropriate other sources might be preferred such as induction lighting. With an eye on the future perhaps it will be plasma light sources next.

Design process

The role of the lighting designer is to understand specific requirements and to detail lighting levels accordingly to maintain a consistent character and style across London.

When working on the TLRN, expert advice should always be sought from TfL Engineering to ensure the lighting design is appropriate for the street, conforms with the relevant British Standards, our own particular requirements, and industry recognised codes of safe and or best practice (for example, ILP and HSE guidance).

Lighting levels

Lighting schemes will be designed to BS 5489-1:2013 and CIE115 or later revisions and include a site specific risk assessment. Junction side road entry areas should also be similarly designed. This is anticipated to result in the majority of our roads being lit to lighting classes of ME3 and profiled to ME4 during the hours of darkness. Profiled lighting levels will be uniformly applied within 'logical groups' which will be managed over time by our CMS. Each logical group will predominantly lie between significant junctions, have consistent physical characteristics, and carry similar traffic volumes (including pedestrian traffic). Colour temperature (correlated) will be 'neutral white' (4,000K).

New street lighting on the TLRN

- Must be compatible with our CMS (incorporating digital addressable lighting interface, DALI, or wireless management and control, WiMAC, ballast)
- Must meet our standards and expectations
- Footbridges and subways should also be illuminated in accordance with BS 5489, BS EN 13201 and CIE115. The use of 'blacklights' in subways to deter drug misuse is not advocated

Materials

It is an objective to rationalise the range of luminaires installed, acknowledging that a Best Value lighting solution for the network as a whole should take priority over the Best Value solution for any individual location as a too localised view can result in management of the lighting asset as a whole being over complex. We therefore look to limit the number of products used and deploy just those with best overall performance.

Materials used on the TLRN must be compatible with the TfL Highway Specification. Functional but aesthetically pleasing equipment is preferred. Designers may request an exception to the palette in special circumstances such as in conservation areas. We do not recommend 'mock heritage' styles but wherever practicable will endeavour to maintain all genuine heritage lighting units. However, consideration to special lighting requirements based on the local context will be given on a case-by-case basis.

Lighting columns

Lighting columns may be conical or stepped tubular (site specific basis), must conform to BS EN 40 and as a standard be specified to accommodate a sign plate of 500 square millimetres. However, consideration for the column specification will be necessary if additional attachments such as banners, hanging baskets, CCTV cameras, etc. are required. Stepped tubular columns are generally confined to higher speed roads. Steel columns are to be finished in accordance with G2a or similar approved with generally a final coat of black (RAL9005) or in some locations signal grey (RAL7004). Aluminium columns are to be left bare or anodised where required.

Columns in vulnerable locations or where foundation difficulties are encountered may be installed in retention sockets subsequent to approval. Retention sockets may also be approved for some illuminated signs and are generally used to secure hooped bollards.

The recommended column set-back from the carriageway kerb face is defined by speed limits:

- Speed limits up to 30mph – column set-back 450mm minimum
- Speed limits above 40mph – column set-back 650mm minimum
- Alternative set-backs according to site specific requirements

Lighting column layouts should be in accordance with the site specific design risk assessment, be sympathetic to the local environment, and include considerations for illumination and maintenance requirements. Street clutter should be reduced by minimising the number of assets across a scheme.

The lighting design risk assessment may conclude that raise-and-lower columns provide the best option.

Figure 284: Heritage lighting should be preserved



At puffin and toucan crossing locations lighting columns should be positioned to enable primary signal heads and associated pedestrian head pushbuttons to be mounted on the column to reduce street clutter and provide good illumination at the crossing point.

Lighting columns should be positioned away from mature and newly planted trees and roots in accordance with NJUG guidance and also to

Figure 285: Example of a stepped tubular column



Figure 286: Example of a conical column



maintain lighting performance. The location of luminaires and column mounting height should be adjusted where tree canopies are low or designed away from trees where possible.

Where proposed lighting schemes are within residential areas lighting columns are to be located at property boundaries and gable centres of properties where possible.

When working on the TLRN:

- Where foundation difficulties necessitate the use of other non-standard foundations these should be in accordance with HSE guidance and again, only after approval from ourselves
- Columns should not be located in central reserves unless agreed otherwise with ourselves

Bracket arms

Bracket arms should only be fitted when required to achieve photometric performance or aesthetic objectives. They should coordinate with the form and proportion of the column with no change of size or 'step'. The outreach length is to be no more than 15 per cent of the column mounting height.

Wall-mounted lighting

Where the highway layout and building facades are appropriate wall-mounted lighting should be considered to minimise street clutter. However, wall-mounted lighting and columns should not be mixed on any street section. Please refer to the Code of Practice for Affixing Traffic Signs and Street Lighting to Buildings in London (2015) for further information.

- Wall-mounted equipment and electrical cables are to be discreet and in keeping with the building character
- For listed buildings consultation with the local planning authority is essential and adequate lead-in time must be programmed for Listed Building Consent
- Feeder pillars should be positioned in line with buildings or with the back of the footway to avoid visual and physical obstruction
- Please refer to the London Local Authorities and Transport for London Act (2003) for further information

High-mast and catenary lighting

Specialised mounting arrangements such as high-mast lighting and catenary lighting must be discussed and approved by TfL Engineering.

Luminaires

Luminaires must conform to the relevant British Standards (for example, BS EN 60598 and BS EN 62722, etc) and demonstrate optimum performance for their intended use.

The luminaire form and shape should not be obtrusive nor out of character with the general street scene.

Any electrical load installed on the TLRN such as a luminaire must have an appropriate ELEXON charge code to permit correct energy settlement.

Figure 287: CMS is used to control lighting levels throughout the hours of darkness



The luminaire must be oriented in accordance with the manufacturer's recommendation (for example to avoid glare). Our preference is for luminous intensity classes of G6 unless otherwise agreed by TfL Engineering.

Control of light pollution

Light pollution or obtrusive light must be avoided. The following lighting conditions are to be avoided:

- High light intensity in an inappropriate location
- Poorly positioned or oriented luminaires
- Undesirable highway lighting spilling out on to the surrounding environment
- Uplighters – uplighting may only be used with the specific consent of TfL
- Tree or invasive building illumination

Intrusive glare should be controlled by complying with BS 5489 and BS EN 13201 standards.

All street lighting on the TLRN should comply with obtrusive light limitations for exterior lighting contained in the Guidance Notes for the Reduction of Obtrusive Light published by the Institution of Lighting Professionals.

Electrical

Where lighting columns are serviced by a distribution network operator (DNO) supply, a secondary isolator is to be fitted in the column base compartment in order that electrical isolation can be safely achieved without the need to touch the DNO cut-out.

Independent connection providers can be used to help reduce delays in scheme works, approvals may be obtained via TfL Engineering.

All electrical installations must be installed and maintained in accordance with BS 7671 and BS 7430.

Good practice and the reduction of street clutter

We are determined to reduce the amount of street furniture that might confront all road users, therefore street lighting columns might also be employed in supporting, for example:

- Traffic signals
- Crossing controls
- Footway luminaires
- Trixi safety mirrors
- CCTV cameras
- Bus flags and timetables (subject to approval of TfL Buses)
- WiFi communications

Litter bins

Any requirement to mount such equipment on a TfL lighting asset first needs to be approved by ourselves to ensure that the specification and structural integrity of the asset is suitable to support the additional load and windage. Requests to mount equipment such as banners, flower baskets and festive lighting are covered by our highway licence arrangement.

Traffic control equipment such as signals and CCTV are placed in specific positions to ensure that the aspects are readily visible and that pedestrians can access push button units or the necessary view is provided. For these reasons, where it is proposed to install traffic control

Figure 288: Trixi mirrors are used by motorists to see their blind spots at junctions



equipment on lamp columns the street lighting designer should contact the relevant system designer to first determine the position of lamp columns and then locate the remaining street lighting around these positions.

Banners and advertising

Banners attached to existing street furniture and equipment such as lighting can provide an effective way of providing temporary signage or advertisement with minimal additional clutter and is controlled by licence.

The banner may be provided where the promoter can demonstrate that:

- The existing column can take the weight of the banner
- The fixings match the colour of the column
- The banners and fixings are removed within an agreed timeframe and with no damage caused to the permanent street furniture
- The banner and fixings do not cause road safety or visibility concerns

Advertising should be integrated within the urban realm so as to not impinge on pedestrian movement or impact on the overall quality of the streetscape.

The content of the advertising should comply with our conditions for the acceptance of advertising. These conditions are also used to control the artwork displayed on London Underground and buses.

Figure 289: Lamp columns can be used as a wayfinding assistant or to add to local character



Figure 290: Combined lighting column and signal head



Illuminated signs and bollards

Illuminated signs and bollards are to be specified and installed in accordance with current TSRGD requirements.

Feature lighting

Although the primary purpose of TfL road lighting is to illuminate the carriageway and the footpaths, consideration is also given for ensuring a pleasing aesthetic appearance. Requests for additional feature lighting will be considered on a case-by-case basis.

Silent Lights by Urban Matter New York City, USA

Playful lighting that responds to sound as vehicles pass overhead

Key functions

Opportunity

The challenge for Urban Matter was to transform the area under the Brooklyn-Queens Expressway in New York.

The underpass sits in a semi-industrial landscape surrounded by heavy motorway traffic. The pedestrian path is empty, dark, intimidating and avoided by locals.

Benefits

The spectacle provides a playful way of lighting the space and also gives a sense of safety at night. The 'gates' act as a wayfinding device to define a pathway at human scale across what would otherwise be a non-place.

Implementation

To create Silent Lights, a series of sensory gates were installed. These use sensors to respond to the noise of the traffic above. Coloured lights illuminate sequentially as vehicles pass overhead.



Image courtesy of Flickr/triebensee



Image courtesy of Urban Matter Inc.

Applying in London

This has the potential to be delivered in similarly forgotten urban underpass locations, such as the A12 through Hackney.

Hyde Park Corner subway London, UK

Redevelopment of vandalised subway using innovative lighting systems

Key functions

Opportunity

The Hyde Park Corner subway is located near the Lanesborough Hotel. Repeated vandalism of existing wall-mounted lights meant that a new vandal resistant lighting solution was needed to re-establish a safe environment.

Benefits

Careful detailing and well-placed lighting led to an atmosphere that was simultaneously calm and safe. The new lighting is attractive, discreet and much less susceptible to vandalism.

The handrails were painted bronze to match surrounding street furniture. Stonemasons were commissioned to replace the damaged stonework using artificially aged stone to ensure the new stone did not look out of place.

Despite its relatively high cost, this redevelopment was very well received.



Image courtesy of DW Windsor ©

Implementation

LED lighting was fitted under handrails; the heat from LED lighting made the handrails pleasantly warm. The lighting levels were adjusted to be brighter leading into the subway, creating an aesthetically pleasing atmosphere.

Applying in London

The usual preference in London is to remove subways; however, when they are retained, this example shows how they can be made calm, attractive and safe.

Blackfriars Underpass London, UK

Using innovative lighting technology to reduce maintenance costs

Key functions

Opportunity

Closing the Blackfriars Underpass for lighting maintenance every 18 months was an expensive and disruptive affair that damaged TfL's reputation.

Benefits

The ingress protection combined with the reduced maintenance of LED lighting makes the new system significantly more robust, and has reducing planned and unplanned maintenance.

Implementation

Using the limited space available, a new LED lighting system was installed; a system used previously in Australian train carriages and extremely resistant to dirt and water ingress.

A specialised diffuser was made to control the lighting within the underpass and ensured compliance with highway regulations.



Applying in London

The technology would be advisable anywhere where maintenance is a costly and complicated issue.

Additional Information

British Standards:

All lighting schemes on the TLRN must meet the relevant British Standard requirements including but not exclusively:

BS 5489: Code of practice for the design of road lighting

BS EN 13201: Road lighting

BS EN 40: Lighting columns

PD 6547: Guidance on the use of BS EN 40-3-1 and BS EN 40-3-3

BS 7671: Requirements for Electrical Installations

BS 7430: Code of practice for protective earthing of electrical installations

Department of Energy & Climate Change:

CRC Energy Efficiency Scheme (Amendment) Order, 2014

ELEXON:

Charge codes and switch regimes: https://www.elexon.co.uk/reference/technical-operations/unmetered-supplies/charge-codes-and-switch-regimes/

Greater London Authority:

The Mayor's Transport Strategy, 2010

The Mayor's Climate Change Mitigation and Energy Strategy, 2011

Health and Safety Executive:

Avoiding danger from overhead power lines

Avoiding danger from underground services

Risks associated with working on or near lamp columns with non-standard roots during excavation works, 2010

International Commission on Illumination:

CIE 115: Lighting of Roads for Motor and Pedestrian Traffic, 2010

Institution of Lighting Professionals:

All lighting on the TLRN should meet the requirements of industry-recognised codes of best and/or safe practice such as those recommended by the Institution of Lighting Professionals' Technical Reports and Guidance Notes including but not exclusively: Guidance Notes for the Reduction of Obtrusive Light

Bats and Lighting in the UK

Code of Practice for Electrical Safety in Highway Electrical Operations

Code of Practice for Variable Lighting Levels for Highways

Guidance Notes for the Reduction of Obtrusive Light GN01, 2011

Managing a Vital Asset: Lighting Supports

Legislation:

Climate Change Act 2008

London Councils

Code of Practice for Affixing Traffic Signs and Street Lighting to Buildings in London (June 2015)

Transport for London

Highway Licensing and Other Consents, 2011: https://www.tfl.gov.uk/info-for/urban-planning-and-construction/highway-licences

13.5 Leftover spaces

Unplanned leftover spaces can have a significant detrimental visual impact on London's streetscape. These neglected spaces may emerge organically as marginal underdeveloped pockets of land at the interface of planning boundaries, or can be the by-product of major developments which failed to integrate well with the surrounding urban fabric. In London this is most common where major highways cut across the landscape and leave fragmented areas adjacent to the roadside or beneath flyovers.

Often visible from the road network these spaces may not be easily accessible or become fenced off as unattractive residual spaces that have been designed as an after thought or not designed at all.

Figure 291: Spaces on the network which appear to be uncared for should be targeted for reinvigoration



They are not so much forgotten urban spaces, as areas of land that were never used in the first place.

Typically these spaces are not managed by the highway authority and can become overgrown, strewn with litter or may exist in isolation as an unattractive and polluted urban void.

Unplanned and poorly maintained spaces can create negative spatial implications, similar to the broken window effect. We recognise that while these spaces may currently exist as areas of neglect, many of them offer considerable potential as places of opportunity.

Strategy

Spaces should be identified adjacent to the road network which may be able to provide additional amenity, environmental or aesthetic benefits for the local area and the network as a whole. Uplift of leftover spaces should not be planned in isolation, but should encompass a wider strategy of improving leftover spaces along a designated route.

Designers are encouraged to establish baseline conditions to ascertain how the space is used, if at all, and identify opportunities which can contribute to wider environmental and socio-economic strategies in the All London Green Grid framework and London Plan. Assessments may include using the Pedestrian Environment Review System (PERS) auditing process to establish how the leftover space adversely impacts on the walking environment. Please contact our streetscape manager when these spaces are located on the TLRN at streetscapeguidance@tfl.gov.uk.

Context

Many of these leftover spaces are not readily accessible by foot and so designers should consider the role that these spaces can provide at a local and citywide level.

As new developments come forward in adjoining parcels of land, leftover spaces may emerge as viable opportunity spaces; as potential links or in some cases, new public spaces or development sites.

Where major street improvements are proposed, designers should be conscious of the surrounding boundary interface to ensure that any new surfacing or planting treatment is integrated with adjoining areas.

Design interventions

All identified spaces should be mapped, regardless of whether an intervention is to be proposed. Any space which has been identified as leftover should be assessed to determine the potential for intervention.

Together with the local authorities, we are encouraged to work in partnership to strategise and deliver site specific design interventions which look to support wider economic, social and environmental strategies.

Design teams should respond to the constraints of the existing space and provide opportunities which are site specific. Interventions may include, but not be limited to, the following options:

1. Improve management and maintenance

Some of the most dramatic changes to the quality of our roads can be achieved by simple changes to existing maintenance regimes.

2. Improve access

Public space is just that. It is by definition open and accessible to all. There should therefore be a presumption in favour of public ownership and adoption. Unless there are specific reasons against this for safety or other concerns.

3. Improve amenity

Greening

All highway landscape improvement proposals should be practical, feasible and sustainable and promoters should work with our arboriculture and landscape team to identify opportunities and management strategies for the Green Estate.

Scrubland can provide a valuable ecological function in the urban landscape. Existing areas of green infrastructure planting should generally be retained, except where a safety inspection identifies a need for remedial work.

Lighting

Improvements in lighting should be considered for spaces which have existing problems in visibility and perceived security. Good lighting can encourage more people to use leftover spaces and can complement other connectivity and aesthetic improvements across the area.

Temporary art installations

Public art may be considered for leftover spaces which are well overlooked and relatively well connected with a reduced risk of vandalism. Installations that are locally resonant or support local talent are preferred.

4. Reimagine the space

A suite of measures could be introduced together to help transform a space into a destination in itself. This may include creating new uses for the space, such as community and play facilities, places to live or commissioning artwork. Proposals of this nature will require community support, such that any design for a new public space provides for the local area.

Figure 292: Wild flowers planted next to the carriageway



Figure 293: A bridge undercroft beautifully clad in metal sheets and gabion cages



Figure 294: Anthony Gormley public exhibition 'Event Horizon'



St Paul's Churchyard London, UK

Repurposing space for public use

Key functions

Opportunity

A large part of St Paul's Churchyard was once a coach park but has since been transformed into a vibrant public square.

Benefits

The churchyard has been transformed into an open, inviting green space, designed to reflect the curved transept of the cathedral and provide a high quality welcoming setting for the new City Information Centre.

Implementation

A section of Carter Lane, between Godliman Street and Cannon Street, was closed, and a larger public space was provided by relocating the coach parking and replacing it with green space.





Applying in London

Schemes such as this could easily be implemented in other locations as part of a wider project.

Underpass Park
Toronto, Canada

Transforming derelict space under and around three flyovers into a vibrant community space

Key functions

Opportunity

Toronto is dominated by elevated motorways. These create physical and psychological barriers between neighbourhoods. To reconnect communities and create more public space, land underneath a flyover was used to create a park.

Benefits

This project has embraced the concrete beams and columns of the surrounding flyovers to create a welcoming environment. It connects two adjacent neighbourhoods and has the potential to act as a catalyst for regeneration in the area.

Implementation

The park was designed to appeal to all elements of the community through the inclusion of a playground, skate park, basketball courts, trees and public art. A large, flexible community space is the focal point for the park and is used for public events, such as markets and festivals.

Applying in London

This has potential for urban areas which are well-connected but bleak and underused.







Images courtesy of Waterfront Toronto

13.6 Pocket parks

The term 'pocket park' can be used to describe small spaces in the public realm that can be greened to offer an area for rest or recreation. Pocket parks can challenge the common perception of what a park can be. They can range from the traditional town centre green, to making better use of unusual spaces, such as underused parking spaces, roof tops, canal banks, or uninspiring green spaces associated with bus stops or road junctions. Pocket parks can also be created as 'meanwhile spaces' giving a temporary use to an otherwise underused piece of land, perhaps in the early stages of the development process. They can often be created at relatively low cost and with short delivery times.

The key principles of pocket parks are that they are:

- Publicly accessible
- Provide opportunity for local communities to enjoy outdoor space
- Encourage healthy living
- Help build social cohesion through providing opportunity for community gardening
- Recreational
- Volunteering

In 2012 the Mayor of London launched a two-year Pocket Parks Programme with the aim to create or improve 100 pocket parks across London. The programme promoted the principles of pocket parks through provision of grants to local authorities, housing associations, and community groups, to enable them to identify, create, design, and deliver 100 parks.

The Mayor's pocket parks are enhancing underused amenity green space that often provides little ecological or social value. Improvements on these sites include creating food growing spaces, reimagining play facilities, and creating new landscapes that promote sustainable urban drainage and improve the local ecology.

The concept of pocket parks has been embraced by the public and community groups and their creation should be considered as integral to public realm improvement projects.

Additional information

Greater London Authority:
Pocket Parks Prospectus:
http://www.london.gov.uk/sites/default/files/Pocket%20Parks%20Prospectus_1.pdf

Pocket Parks Programme:
http://www.london.gov.uk/priorities/environment/greening-london/improving-londons-parks-green-spaces/pocket-parks

Figure 295: Van Gogh Walk



The Edible Bus Stop®
London, UK

Making the most of spaces through urban greening

Key functions







Images courtesy of © 2014 The Edible Bus Stop®

Opportunity

There are many small underused public spaces across London, that if enhanced through urban greening, could help to make London a more pleasant city in which to live and work. The Edible Bus Stop®, an urban design group, saw an opportunity to transform a small poorly managed patch of amenity grass, into a new public garden maintained and managed by the community. In 2013, with help from London Borough of Lambeth and funding from the Mayor of London, the group designed and delivered the Mayor's first pocket park on Landor Road, Lambeth.

Benefits

Changing underused grey spaces into dynamic green spaces through clever design and planting can improve public perception of the public realm, and foster community cohesion and civic pride. Other benefits can include food growing and enhancing biodiversity. There are also well-documented links between making the public realm greener and more pleasant and boosting the local economy.

Implementation

The Edible Bus Stop® undertook extensive community outreach at every stage of the project, galvanising support from the outset. The group reimagined the entire area; creating large robust planting beds out of discarded granite kerbstones; adding new bespoke oak seating, and with the community planted edible plants, including herbs, strawberries, five fruit trees and rainbow chard. It has given local residents a space to come together and enjoy, and has encouraged them to take ownership, volunteer to help maintain the space, and grow what they wish. It has given the street an asset, making the space a place and the streetscape more pleasant and friendly.

Applying in London

One of The Edible Bus Stop's® ambitions is to create a series of small green spaces along transport routes starting with the length of the 322 bus route. Working with other local community groups, it has already applied the concept in spaces in West Norwood and Crystal Palace, on the 322 route. It hopes to set a precedent with its Edible Bus Route and roll out the concept across London's transport network and beyond. The approach is transferable to thousands of other underused, amenity spaces scattered across London's streetscapes. Small-scale improvements, as demonstrated at Landor Road Pocket Park, have created positive impacts on the local community's wellbeing and contributed to a cleaner, greener and friendlier city.

Parklets
San Francisco, USA

Introduction of small urban parks in underused car parking spaces

Key functions

Opportunity

The distribution of public open space is often unequal in urban contexts. Where there a shortage of public open space or the quality of the public realm is poor the creative use of space, such as parklets, should be encouraged.

Benefits

San Francisco's Parklet Program works to convert underused parking spaces into publicly accessible open spaces called parklets. These are generally installed next to the footway thereby extending the area of useable space for pedestrians as well as providing a range of facilities including seating, cycle racks and landscaping.

Implementation

The programme has sought to install parklets where there is a notable lack of public open space or where existing footway width is highly constrained. Parklets are designed to be permanent, temporary or seasonal structures which are financed and maintained in collaboration with local councils, business owners and non-profit community organisations.

Applying in London

London's Pocket Parks Programme has already transformed underused or derelict spaces and repurposed them for increased green space. The introduction of parklets could seek to improve constrained footways.

Derbyshire Street Pocket Park London

Creation of small urban parks in underused streets and public realm

Key functions







Images courtesy of Greysmith Associates

Opportunity

Providing access to quality open space is always a challenge in the most densely developed parts of the urban environment. There are many competing pressures on the public realm and creating green space requires thoughtful design and creative use of space. The eastern end of Derbyshire Street, Bethnal Green, was a dead-end road with only one function – space for 12 car parking bays. These were used infrequently; consequently the space created conditions that encouraged antisocial behaviour and fly-tipping.

Benefits

London Borough of Tower Hamlets sought to provide environmental and social benefits by transforming the underused space into a pocket park. The design incorporated a cycle path, new seating, green-roof covered cycle racks and bin stores, a rain garden and a defined area for café tables and chairs. Bespoke planters to capture rainwater from the roof of Oxford House, a popular community and arts centre, were designed and provided by Thames Water.

Implementation

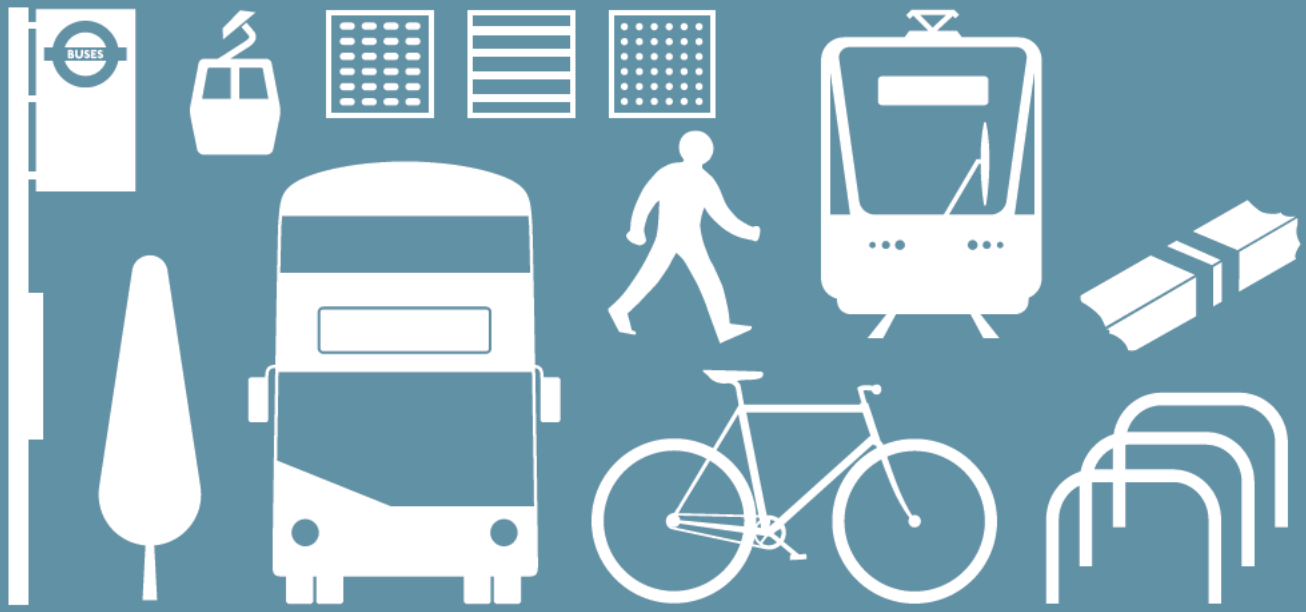
The aim was to recreate an important node for pedestrians and cyclists within a thriving network of streets creating an active place from an unused space. A small section of the adjacent park was also incorporated into the design of the scheme, increasing connectivity as well as improving the opportunity to provide sustainable urban drainage. Funding for the project was provided by the Mayor of London's pocket park initiative and London Borough of Tower Hamlets.

Applying in London

Derbyshire Street Pocket Park is an excellent example of how the conversion of an underused grey space into a quality green one can provide a suite of improvements that address issues affecting many parts of London, for example, tackling antisocial behaviour or coping with areas prone to flooding. Each of the interventions delivered here can be applied in similar spaces across London, creating a mosaic of small urban spaces which are valued by local people and deliver more strategic environmental benefits through cumulative impact.

Part E Transport interchanges

14.1 Vision 314
14.2 Street interchanges 314
14.3 Transport mode specific design considerations 317
14.4 Rail interchanges 318
14.5 On-highway bus station interchanges 319
14.6 Tram interchanges 320
14.7 London River Services interchanges 322
14.8 Taxi ranks 323
14.9 Cycle parking hubs 325



14.1 Vision

The interface between a transport hub and the street is an essential part of the streetscape experience. It needs to provide a seamless journey and a clear transition for passengers using transport facilities, accommodate the needs of the station and demonstrate good practice streetscape design principles.

Figure 296: Wapping station interchange between buses and the station entrance



14.2 Street interchanges

The street almost always acts as an interchange zone, an area encompassing one or more interchange facilities creating a multi modal hub, and public space. It needs to fulfil several functions to provide a clear transition for passengers. Interchange zones need to facilitate convenient and safe pedestrian movement between different transport modes and allow for the efficient operation of public transport services.

Stations within the context of Streetscape Guidance are defined as any transport hub used to access public transport, which may or may not include infrastructure located directly on the road network. This includes:

- Rail stations – London Underground, London Overground, Docklands Light Railway and National Rail
- Bus stations – infrastructure which is provided on-carriageway
- Tram stops – operated by London Trams
- Piers – operated by London River Services or others
- Taxi ranks
- Cycle parking hubs

Our Interchange Best Practice Guidelines (2009) should be referred to as a general guide to improving quality and efficiency, and Station Public Realm Design Guidance (2015) referred to when defining the design approach for the station's public realm. Streetscape Guidance should be referred to when detailing the materials and their application from any station entrance that directly faces the street.

Station public realm

Stations and the spaces around them are important focal points for an area with the potential to become a destination in its own right, so any design should look to embrace the local character and sense of place, while providing a legible and consistent streetscape, linking effectively with the surrounding street network.

Figure 297: Wimbledon station forecourt provides seating, cycle parking, public art, taxi rank, and bus interchange



Not every station will include these spaces, generally referred to as a forecourt, a defined area which connects the station entrance to the streetscape, however, where they do occur the following should be accounted for:

- The space should be flexible such that it can respond to daily trends in pedestrian flows and accommodate different uses at different times. This may include temporary uses of space during quieter periods. The station forecourt should work as a cohesive and legible whole, with clear sightlines and well-defined transport entrances
- Designers should consider the context, proportions of the space and the degree of enclosure, when selecting materials and placing furniture within the forecourt. Please refer to the section 'High quality footways' in this guidance for further information
- Where retail units front on to the forecourt, frontages should be visually cohesive, with outdoor seating managed in designated licensed areas

Figure 298: Temporary table tennis installation at King's Cross/St. Pancras station



Figure 299: Legible London signage should be placed near an interchange point



Wayfinding

Information requirements vary depending on the stage in the passengers journey. The provision of comprehensive and consistent wayfinding information across the interchange should be provided to assist navigation. Please refer to Station Public Realm Design Guidance (2015) for further information. Consideration should be given to:

- Appropriate placement of transport infrastructure, such as bus stops, tram stops, kiosks and cycle hubs should aid natural wayfinding and minimise the need for signage when onward travel infrastructure is located within a direct line of sight from an alighting area
- Where direct line of sight to an onward journey mode is not achieved, routes should be simple with signage provided at key decision points. Signage should be rationalised to reduce clutter. Refer to 'Pedestrian wayfinding' and 'Traffic signs' in this guidance, and London Underground Signs manual (Issue 4, 2002) for further information

Footways

Surface materials can be used as a navigational tool and to communicate a change in use. A change in surface materials helps to demarcate the limits of the interchange zone or highlight where there will likely be a greater or different type of pedestrian presence. Each design response should be site specific and consider its function, performance and context. The following examples are potential approaches to the treatment of the footway:

- A consistent approach to paving the footway in front of the station should be used to maintain visual continuity with the surrounding streetscape. Where designers are looking to extend forecourt paving across the footway SDRG approval is required

Figure 300: Green Park Tube station entrance paving has a distinct design used as a 'welcome mat' into the station



- Non-standard surface materials require SDRG approval but may be considered for use on the footway outside a station if the design intent is to visually unify the street and interchange zone. This may be useful in larger forecourt settings where a consistency of material can reinforce the station setting and better relate to the surrounding architecture
- Footways should be designed to accommodate peak pedestrian flows, but be flexible so that they also work at quiet times. Refer to Pedestrian Comfort Guidance for London (2010) for further details

Carriageways

- Special consideration to surface materials is required at interchange points due to frequent and heavy use. All materials and treatments must be robust and able to withstand anticipated use

Figure 301: Bus interchange with a 140mm kerb upstand



- Clear delineation in surface materials and kerb heights are recommended in interchange zones between footways and carriageway. An upstand of 140mm is recommended in most cases
- Containment kerbs may be required where a safety audit has identified a risk of vehicle overrun on to the footway. Please refer to 'Kerbs' for further information
- Signalised crossings should be provided on primary pedestrian desire lines at the entrance to the station to allow people less confident to cross. Please refer to 'Crossings' for further information

Street furniture

Street furniture can be used to reinforce different public realm functions, particularly with regard to pedestrian movement: stationary activity can be encouraged by providing seating away from major desire lines; or trees can be used to reinforce primary walking routes towards the station.

The placement of street furniture on the footway adjacent to an entrance or forecourt area should allow for complex pedestrian movements, as pedestrian desire lines will likely not just be along the street. It should also be recognised that people will need more space to stop, orientate themselves and wait for others.

- The standard Streetscape Guidance furniture placement design principles still apply (refer to 'Footway amenities' and 'Safety and functionality'), however, back of footway furniture should be carefully considered to ensure adequate permeability between kerb edge services, such as buses and taxis, and the station entrance. The placement of street furniture should not hinder maintenance activities
- Large cycle hubs may be required to support station facilities and these should be sited in a convenient location which does not impinge on footway space. For normal cycle provision please see 'Cycle parking'. Designers should consider how cyclists will access cycle parking facilities if not at the kerb edge, to ensure that they do not inadvertently create a shared space to the detriment of pedestrian movements. Cycle parking must not create a barrier therefore short strips of no more than six racks should be provided
- Passenger information, street furniture and signage should all be coordinated in furniture zones, with structures or at the back of footway to minimise clutter

Figure 302: Emirates Air Line Greenwich Peninsula station where stone plinths are used as a security measure and a seating feature



Security

The approach to security should be to firstly design out the likelihood of crime through passive measures and good quality design. The layout should ensure good natural surveillance, be well-lit and promote a high sense of personal security by avoiding the creation of blind spots or dark corners. Careful design, selection and placement of street furniture can create passive measures that prevent and discourage crime from occurring without affecting the overall character of a place. All aspects of the design must comply with Section 17 of the Crime and Disorder Act.

Overt use of CCTV can help in some situations to deter crime, but should not be relied upon in itself due to its relation to fear of crime. Cameras should be placed and merged with adjacent street furniture to minimise visual clutter. Refer to 'Roadside cameras and CCTV' for further information.

Where security bollards are required other furniture such as reinforced seating should be considered to provide greater multifunctional value and help to reduce street clutter. Please note that where street furniture is intended to be used as a security measure, it must first be approved by the Centre for the Protection of National Infrastructure. Security bollards should be considered as a last resort where vehicle incursion may occur and carefully detailed to minimise their use. Refer to 'Barrier free footways' for further information.

- Footways and waiting areas should be visually permeable to enable adequate passive surveillance

Additional information

Transport for London:

Accessible Bus Stop Design Guidance, 2015

London Underground Signs manual, 2002

Pedestrian Comfort Guidance for London, 2010

Station Public Realm Design Guidance, 2015

London Underground Station Design Idiom, 2015

14.3 Transport mode specific design considerations

The following section outlines mode specific design considerations that should be read alongside Station Public Realm Design Guidance.

14.4 Rail interchanges

A large number of major rail stations front directly on to the TLRN including London Euston, London King's Cross and Waterloo, as well as numerous London Underground, London Overground, Docklands Light Railway and National Rail stations.

Designing the interface of the street with these stations is crucially important to maintaining the quality and continuity of the streetscape at some of London's busiest transport nodes.

Detailed guidance

Footways

There are several general approaches to surface treatments typically used at station entrances that treat the entrance as:

An 'entrance mat' – using a visually different paving material directly surrounding the station entrance to highlight the entrance. This approach tends not to be used in new stations, but is commonly seen at stations that are listed or in a conservation area. If considering this approach please seek the approval of the SDRG.

A distinct space – using a distinct urban realm treatment in the forecourt of the station to distinguish it as a separate space from that of the street. This approach can be extended across the footway or stop at the edge of the footway.

Figure 303: King's Cross station forecourt uses stone plinths as a security measure



If considering this approach please seek the approval of the SDRG.

Part of the street – using the same material as the footway up to and perhaps into the station entrance. This is a common approach when the station entrance is directly on the street and there is little or no forecourt space.

Streetscape Guidance seeks a consistent approach to footway paving as seen in 'High quality footways' and 'Footway amenities'. When considering an alternative approach, please seek the approval of the SDRG.

Street furniture

- Station Public Realm Design Guidance provides detail on when and where it may be appropriate to locate street furniture. If street furniture will be included at the station entrance or forecourt, please follow the guidance set out in:
- 'Ambience'
- 'Footway amenities'
- 'Safety and functionality'

Large cycle hubs, refer to 'Cycle parking hubs', may be required to support rail station facilities and these should be located in a convenient location which does not on impede on footway space. Designers should consider how cyclists will access the cycle parking facility if it is not at the kerb edge, to ensure that they do not inadvertently create a shared space to the detriment of pedestrian movements.

Additional information

Transport for London:

Station Public Realm Design Guidance, 2015

Interchange Best Practice Guidelines, 2009

London Underground Station Design Idiom, 2015

Department for Transport:

Security in Design of Stations (SIDOS) Guide, 2012

14.5 On-highway bus station interchanges

Most of London's major bus stations are integrated with other public transport modes, in particular London Underground. The interchange experience is therefore a key consideration in delivering an efficient and beautiful public realm which acts as a pleasing transitional space between transport modes.

Streetscape Guidance does not provide specific details on bus station design; rather it identifies the key design considerations for ensuring successful urban integration of the bus station with the adjoining road network, and clarifies the aspirations for maintaining the quality and character of the streetscape across the bus station frontage.

Figure 304: Bus interchanges happen both on and off the highway



Figure 305: On-street bus interchanges need to provide for the safe passage of cyclists and vehicles



General considerations

Bus interchanges accommodate a high frequency of buses and a large volume of people. Therefore, bus interchanges should aim to provide clear delineation between waiting areas and movement corridors to avoid congestion and ensure the safety of all users.

Provision for cycling is a priority that should be designed in for both on-carriageway facilities and cycle parking. Different regulations apply to bus station that are off-highway.

The design of the station buildings and the configuration/provision of bus stops will depend on site-specific operational and spatial characteristics, and will always require specialist architectural and highways advice. Our Bus Infrastructure team should always be consulted regarding any street improvement project adjoining a bus station or any aspect of a TfL bus station.

Detailed guidance

Many major bus interchanges will occur on the highway road network where passengers can transfer to another mode of transport like rail or Tube. Brixton, Waterloo, King's Cross and Paddington stations are just a few examples of where buses stop on the carriageway at frequent intervals to allow passengers to interchange.

These interchanges are often constrained by narrow footways and active frontages. However, the following considerations can help relieve congestion and create a smooth interchange:

Footways

- Consider the provision of a centre median along the length of an on-carriageway interchange zone to assist passengers with informal crossings. The median should be paved in the same material as the footways and no street furniture should be placed on it
- Provide frequent and wide formal crossings on desire lines; refer to Crossings for further information
- Design teams should use a consistent approach to paving the footway and it should match the material of surrounding footways to maintain visual continuity with the surrounding streetscape
- When designing a forecourt as part of an interchange that is public space, designers should first consider the opportunity to create a place when reviewing the approved

palette of materials in this guidance. Bespoke materials should only be considered where a strong case can be made as to their value in responding to the character of the space and the surrounding architecture. This will require approval by the SDRG

- Where a non-standard material has been specified, designers should be especially careful in detailing the intersection of the bespoke treatment with the standard footway materials used on the TLRN

Street furniture

- Street furniture should be kept to a minimum and equipment and signs should be combined where possible; refer to 'Footway amenities' and 'Safety and functionality' for more information
- Passenger information and bus stop signage should all be coordinated in furniture zones to minimise clutter. Consideration of adjacent frontages when siting bus infrastructure is important and will influence the layout and format of bus stop shelters. Please contact our Bus Infrastructure team and refer to 'Kerbside activity' for further information

Carriageway

- Carriageway surfacing should be carefully considered so as to ensure durability
- Containment kerbs may be required where a safety audit has identified a risk of vehicle overrun on to the footway
- Please be aware of DfT guidance on highway marking

Additional information

Transport for London:

Interchange Best Practice Guidelines, 2009

Accessible Bus Stop Design Guidance, 2015

Station Public Realm Design Guidance, 2015

14.6 Tram interchanges

Tramlink provides 28km of rapid, street level and off-carriageway services across central Croydon, from Wimbledon to New Addington, Elmers End and Beckenham Junction. Tramlink is a fully integrated public transport service and connects with numerous bus routes, seven mainline rail stations and the London Underground.

Powered by electricity, trams do not emit fumes and so provide a greener public transport solution than motor vehicles. They do however require extensive infrastructure for operation including rail tracks within the carriageway, overhead power lines and raised platforms. Any proposed extension or changes to the route should consider the visual impact on the streetscape, in particular, where possible building fixings should

Figure 306: Elmers End tram stop



be used to support the overhead. Where this is not possible special consideration should be given to the visual impact that the overhead line supports may have on the urban environment.

London Trams, a division of London Rail, is responsible for maintaining the infrastructure and the vehicles, overseeing the operations of the Tramlink network and for future enhancements to the system. We are committed to maintaining and improving the tram network by providing higher frequency services, without compromising the road network capacity.

Location

- Tram stops may be located within the street environment or off-carriageway and consist of a raised platform, ticket vending machine, Oyster reader, emergency help point, information boards and shelter and seating where space allows
- Tram routes that run within the carriageway either run in mixed traffic or within their own dedicated lanes
- Highway arrangements at on-street stops shall be designed to minimise the speed of traffic through or around the stop. The layout of on-street stops must be designed to minimise the risk of vehicles mounting the platform or hitting the platform edge

Detailed information

Platform widths should be designed to cater for the anticipated volume of pedestrian use.

- The minimum width between tramway edge and any structure should be 1,500mm
- The nominal minimum platform width will be 3,000mm for side platforms and 5,000mm for island platforms
- Side platforms with absolute minimum width of 2,000mm may be considered where pedestrian demand profiles are sufficiently low and designs agreed with London Trams on the basis of risk and value management assessments
- Along the full length of the platform, a single row of lozenge tactile paving should be used to delineate the edge with a contrasting colour
- The kerb height needs to be raised in most instances to 350mm to provide step-free access for boarding the tram

Figure 307: Tram and bus interchange at Centrale shopping centre, Croydon



- Poles to support overhead lines should be setback at least 450mm from the kerb edge. These poles should be considered for mounting other signage or street lighting to reduce clutter, while taking into account the maintenance requirements as strict access arrangements are in place due to overhead lines carrying high voltage
- Signalised pedestrian crossings across the carriageway are not generally required at each end of each platform, however, an uncontrolled crossing point should be provided where the desire lines dictate it
- The provision of a signalised crossing will be dependent on pedestrian desire lines, sightlines and vehicle flows and will be determined using risk assessment and industry guidelines/standards
- Tree plantings should be considered where possible

Additional information

Department for Transport:
Inclusive mobility – A guide to best practice on access to pedestrian and transport infrastructure, 2021

Office of Rail Regulation:
Guidance on Tramways: Railway Safety Publication 2

Transport for London:
Trams Customer Environments

14.7 London River Services interchanges

The road network and London Underground stations are often adjacent to a number of our piers, including Victoria Embankment adjacent to Blackfriars, Embankment and Westminster piers, and New Ferry Approach and Pier Road serving the Woolwich Ferry terminals.

The design of the public realm in these locations generally requires minimal alterations to standard arrangements. For most pier locations, the majority of the supporting infrastructure is provided off the highway and on the river.

Figure 308: London River Services' totem and ticket kiosk



Off highway infrastructure includes walkways, waiting rooms and boarding ramps on floating pontoons. Design guidance for these components is detailed in our London River Services: River Infrastructure Guidelines (2014).

Highway provision is generally limited to a single free-standing ticket kiosk, overhead pier signage, free-standing poster frame units and a Legible London wayfinding totem.

Ticket kiosk

- Ticket kiosks should be located in close proximity to the pier entrance on a highly visible stretch of footway, line of sight should ideally be maintained to any nearby London Underground stations, bus stops or other major interchanges
- The placement should be a minimum 450mm from the kerb edge, facing in towards the footway so as to encourage queuing away from the carriageway

Figure 309: River pier ticket kiosk



- The building should meet current building regulation requirements
- A minimum unobstructed footway width of 4,000mm should be provided at the ticket kiosk front desk
- Waiting rooms with seating are provided on some piers; however, additional seating may be provided within the footway furniture zone a minimum of 2,000mm from the kiosk, so as to ensure adequate access to the kiosk door
- Temporary queue management barriers may be erected during opening hours if required. The footway should maintain a 2,000mm unobstructed width. After hours, barriers should be stored on the pontoon

Signage

- Ticket kiosk signage should be clear and concise, to minimise the visual impact on the streetscape, while providing sufficient information for passengers
- Tamper proof vinyls and anti-graffiti overlays should be used in all exterior applications where signage is required
- Designers should refer to the bespoke treatments and approved standards in our London River Services: River Infrastructure Guidelines (2014)

Additional information

Transport for London:
London River Services: River Infrastructure Guidelines, 2014

14.8 Taxi ranks

We are responsible for the regulation of taxis and private hire vehicles (PHVs). TfL Taxi and Private Hire is responsible for appointing and revoking all taxi ranks within the London boroughs, other than those located in the City. Taxi ranks within the City of London are not under our jurisdiction, but are appointed and managed by the Commissioner of Police for the City of London.

Figure 310: Taxi rank



Designers should consider the contribution that taxis can provide at interchanges for onward travel and ensure that the placement and design of taxi ranks and set down/pick-up facilities do not impede general traffic flows while remaining convenient and accessible for passengers, particularly for those with mobility impairments. Taxi ranks are particularly important to disabled people or those who have difficulty accessing other transport modes. Taxi ranks may only be used by taxis (Hackney Carriages) and not PHVs which must be pre-booked via a licensed TfL operator. Please refer to the Taxi Ranks at Major Interchanges: Best Practice Guidelines (2003) for information on general design principles of taxi ranks.

Location

Taxi ranks should be located close to transport interchanges and major attractions such as retail areas, bars/restaurants, events, sports stadia and hotels. We can also appoint rest and refreshment ranks to provide a designated space for taxi drivers to take a short break.

Ranks should be positioned with due regard to safety, so that passengers can board from or alight on to the footway from the nearside doors of a taxi. Care needs to be taken with respect to cyclists and cycle routes.

Materials and layout

When designing a taxi rank, a length of 5,000mm per taxi is standard. The size, layout and design of the taxi rank will depend upon several factors but must be located within sightline of the venue they serve and at a suitable distance for the passenger. Please refer to Taxi Ranks at Major Interchanges: Best Practice Guidelines (2003) for further information.

- Taxi ranks should be clearly signed and marked according to the TSRGD manual. Set down and pick up areas should have a minimum kerb height of 140mm to allow easier access for those with mobility impairments and luggage
- Footways adjacent to the taxi rank should have an unobstructed minimum width of 2,000mm for alighting and boarding; sufficient for wheelchairs to manoeuvre and to accommodate access ramps and an additional 1,500mm for pedestrians to bypass the rank
- A formal pedestrian crossing with a dropped kerb or raised table should be located near to the taxi rank to allow for convenient, safe access and to discourage informal crossing in-between taxis. However, taxi ranks should not be on the opposite side of the road to the venue they serve forcing passengers to cross the road before being able to access a taxi
- Seating and shelter should be positioned nearby where space allows

Figure 311: Taxi set down and pick up areas should have a minimum kerb height of 140mm



Road markings and regulations

- Taxi ranks are bays marked with 50mm-wide yellow broken lines on the edge or centre of the carriageway surface and signed in accordance with the TSRGD
- Only licensed taxis are permitted to stop in the areas bounded by the road markings
- For all TfL-appointed taxi ranks on the public highway, a taxi rank order must be completed and this is undertaken by TfL Taxi and Private Hire. If the taxi rank is on the public highway then a Traffic Management Order should also be completed to ensure it can be enforced and this will be carried out by the highway authority

Consultation

TfL Taxi and Private Hire must be consulted in all projects involving taxi ranks to advise on location, design and layout.

Additional information

Statutory instruments:

Traffic Signs Regulations and General Directions, 2002 and 2015

Department for Transport:

Inclusive mobility – A guide to best practice on access to pedestrian and transport infrastructure, 2021

Transport for London:

Taxi Ranks at Major Interchanges: Best Practice Guidelines, 2003

Transport for London appointed taxi ranks, 2014

14.9 Cycle parking hubs

This guidance should be read in conjunction with the London Cycling Design Standards, 2014: Chapter 8.5 – Cycle parking to support different uses. It provides guidance specifically for cycle hubs adjoining the TLRN.

Cycle parking hubs are designed to provide a large number of secure cycle parking spaces in areas of highest demand, while also offering a range of related facilities which may include cycle maintenance, secure long-stay parking and cycle hire.

Hubs are most often located near rail stations but may also be considered for major trip attractors such as shopping centres or landmark buildings. Reliable cycle parking facilities and hubs at stations will become an increasingly important way of supporting cycling as a viable interchange mode for onward travel.

The installation of large cycle parking facilities at stations may be complicated by land ownership and commercial relations. Local authorities are encouraged to work in partnership with landowners and ourselves to provide facilities that can accommodate and support the anticipated future growth in cycling.

Figure 312: Ealing Broadway cycle hub



(Image courtesy of H-B Designs Ltd)

Location

- Where the TLRN adjoins a station forecourt, a cycle parking hub may be considered within the road network boundary, as long as complementary measures are put in place to maintain appropriate unobstructed footway widths. This may include footway widening or decluttering of other street furniture
- As a minimum, footway widths of 3,000mm should be provided adjacent to hubs, to allow for a waiting cyclist to gain access to a facility without blocking the full width of the footway
- Cycle hubs should be located within convenient access of the station entrance, no more than 200 metres away, so that cyclists are less inclined to fly park closer to the entrance
- The location should ensure high levels of natural surveillance, supported by CCTV coverage

Design considerations

- Any new structure should aim to accommodate current summer demand for cycle parking and provide an additional 20 per cent of space where practicable
- The placement should not obstruct existing pedestrian desire lines or create unnecessary conflict between pedestrians and cyclists crossing the footway to access the hub. It may be appropriate to provide a shared use area around the hub, with dropped kerbs to allow for safer, more comfortable cycle access
- For any secured facility, designers should carefully consider the management regime, staffing requirements, tariff rates, and access arrangements, so as to maintain a viable and efficient facility

Detailed Information

- Parking stands should provide two lockable points, so the frame and both wheels of the cycle can be securely fixed, as detailed in 'Cycle parking'
- Gated compounds should allow for 24-hour access
- Any covered structure should ensure a minimum head clearance of 2,400mm. This might be an opportunity to create a structure that responds to its context, and act as a beacon or icon
- Roofs should be sloped so as to reduce the accumulation of debris and discourage antisocial behaviour
- Cycle hub surface materials should respond to the local context. The use of setts should be avoided in favour of 900x600mm slabs or asphalt
- Street furniture must be kept to a minimum to allow for regular and numerous pedestrian and cycle movements (refer to London Cycling Design Standards, 2014)
- Where the cycle hub is located on the footway dropped kerbs should be provided and shared use areas should be considered

Additional information

Transport for London:

London Cycling Design Standards, 2014: Chapter 8 – Cycle parking

Part F Appendix

15.1 List of references..... 328
15.2 List of revisions 333



15.1 List of references

Transport for London:

Accessible Bus Stop Design Guidance, 2015

Bus pre-signal assessment and design guidance – Bus Priority Team technical note BP1/05, July 2005

Bus priority at traffic signals keeps London's buses moving – Selective Vehicle Detection (SVD), 2006

Centreline removal trial, 2014

Cycle Security Plan, 2010

Design Standards for Signal Schemes in London, 2011

Green Estate Management Plan

Guidance on bus intelligence systems, 'Countdown for London'

Guidance on the Assessment of Pedestrian Guardrail, 2012

Highway Licensing and Other Consents, 2011: https://www.tfl.gov.uk/info-for/urban-planning-and-construction/highway-licences

Interchange Best Practice Guidelines, 2009

International Cycle Infrastructure Best Practice Study, 2014

Kerbside loading guidance, 2009

Legible London Design Standards, 2010

London Cycling Design Standards, 2014

London Cycle Hire Scheme Agreement, 2009

London River Services: River Infrastructure Guidelines, 2014

London Underground Station Design Idiom, 2015

London Underground Signs manual, Issue 4, 2002

Network Operating Strategy, 2011

Motorcycle Safety Action Plan, 2014

Pedestrian Comfort Guidance for London, 2010

Station Public Realm Design Guidance, 2015

Surface Transport Panel – Subways, 2009

Traffic calming measures for bus routes – Bus Priority Team technical note BP2/05, September 2005

Transport for London appointed taxi ranks, 2014

Travel in London, Supplementary Report: London Travel Demand Survey, 2011

Taxi Ranks at Major Interchanges: Best Practice Guidelines, 2003

British Standards:

BS EN 40: Lighting columns

BS EN 124: Gully tops and manhole tops for vehicular and pedestrian areas

BS EN 1340:2003 Concrete kerbs

BS EN 1341: Provides guidance on the breaking load for setts

BS EN 1343:2012 Kerbs of natural stone

BS EN 1871: For directly laid materials

BS EN 13108: Bituminous mixtures. Material specifications (BSI, 2010)

BS EN 12899-2: Fixed, vertical road traffic signs. Transilluminated traffic bollards (TTB), 2007

BS EN 13201: Road lighting

BS EN 60598: Luminaires

BS EN 62722: Luminaire performance

BS 4428: Code of practice for general landscape operations

BS 5489: Code of practice for the design of road lighting

BS 5837:2012 Trees in relation to design, demolition and construction – Recommendations (BSI)

BS 7430: Code of practice for protective earthing of electrical installations

BS 7533-6:1999: Pavements constructed with clay, natural stone or concrete pavers

BS 7533: Part 12 provides sub-structure advice for pedestrian areas

BS 7669-3: Guide to the installation, inspection and repair of safety fences

BS 7671: Requirements for Electrical Installations

BS 7903: Guide to selection and use of gully tops and manhole covers for installation within the highway

BS 8301: Drainage

BS 594987: Recommendations for the laying of the various asphalts

PD 6547: Guidance on the use of BS EN 40-3-1 and BS EN 40-3-3

Publicly Available Specifications (PAS) 68 and 69, 2005

Commission for Architecture and the Built Environment (CABE):

Paving the way: How we achieve clean, safe and attractive streets, 2002

Health and Safety Executive:

Avoiding danger from overhead power lines

Avoiding danger from underground services

Risks associated with working on or near lamp columns with non-standard roots during excavation works, 2010

Department for Communities and Local Government:

Outdoor advertisements and signs: a guide for advertisers, 2007

Department of Energy & Climate Change:

CRC Energy Efficiency Scheme (Amendment) Order, 2014

Department for Environment Food & Rural Affairs:

Local Air Quality Management: Technical Guidance, 2009

National Standards for sustainable drainage systems, 2011

Department for Transport:

Delivering the goods: Guidance on delivery restrictions, 2006

Design Guide 003 Note: Tactile Paving

Design Manual for Roads and Bridges, Volume 2 – Highway Structures: Design (Substructures & Special Substructures) Materials

Design Manual for Roads and Bridges: Volume 2, Section 2, Part 4, TD19/85: Safety Fences and Barriers

Design Manual for Roads and Bridges: Volume 2, Section 2, Part 8, TD19/06: Requirement for Road Restraint Systems

Design Manual for Roads and Bridges: Volume 4 – Geotechnics and Drainage

Design Manual for Roads and Bridges, Volume 6, Section 3, TD36/93: Subways for Pedestrians and Pedal Cyclists. Layout and Dimensions

Design Manual for Roads and Bridges, Volume 8, Section 1, TA 84/06: Code of Practice for Traffic Control and Information Systems for All-Purpose Roads

Design Manual for Roads and Bridges, Volume 8, Section 2, Part 2, TD 33/05: The Use of Variable Message Signs on All-Purpose and Motorway Trunk Roads

Inclusive mobility – A guide to best practice on access to pedestrian and transport infrastructure, 2021

Local Transport Note (LTN 1/94): Design and Use of Directional Informatory Signs

Local Transport Note (LTN 1/95): The Assessment of Pedestrian Crossings, 1995

Local Transport Note (LTN 2/95): The Design of Pedestrian Crossings, 1995

Local Transport Note (LTN 1/97): Keeping Buses Moving

Local Transport Note (LTN 1/98): The Installation of Traffic Signals and Associated Equipment

Local Transport Note (LTN 2/09): Pedestrian Guardrailing, 2009

Manual of Contract Documents for Highway Works, Volume 1, Series 400: Road Restraint Systems (Vehicle and Pedestrian)

Manual for Streets, 2007

Guidance on the use of Tactile Paving Surfaces, 2021

Traffic Advisory Leaflet 01/13 (2013): Reducing Sign Clutter

Traffic Advisory Leaflet 2/02: Motorcycle Parking

Traffic Advisory Leaflet 03/13: Traffic bollards and low level traffic signs

Traffic Advisory Leaflet 5/02: Key elements of cycle parking provision

Traffic Advisory Leaflet 5/91: Audible and tactile signal controlled junctions, 1991

Traffic Signs Manual 1982 and 2013

Security in Design of Stations (SIDOS) Guide, 2012

Signing the Way 2011: Traffic Signs Policy Paper

Disabled Persons Transport Advisory Committee:

Inclusive projects, 2003

ELEXON:

Charge codes and switch regimes: https://www.elexon.co.uk/reference/technical-operations/unmetered-supplies/charge-codes-and-switch-regimes/

English Heritage:

Streets for All, 2005

Forestry Commission

Right Trees for a Changing Climate: (www.righttrees4cc.org.uk)

Greater London Authority:

All London Green Grid SPG, 2012

Greenspace Information for Greater London (GiGL) (www.gigl.gov.uk)

Pocket Parks Programme:

http://www.london.gov.uk/priorities/environment/greening-london/improving-londons-parks-green-spaces/pocket-parks

Pocket Parks Prospectus: http://www.london.gov.uk/sites/default/files/Pocket%20Parks%20Prospectus_1.pdf

The Mayor's Climate Change Mitigation and Energy Strategy, 2011

The Mayor's Transport Strategy, 2010

The GLA Group Responsible Procurement Policy, 2008

The London Plan, 2011

Retail in London, 2006

Highways Agency (HA):

Design Manual for Roads and Bridges (DMRB): Volume 10, Environmental Design and Management, HA, Section 3: Landscape Management

DMRB: Volume 10, Environmental Design and Management, HA, Section 0, Part 2: Environmental Functions

DMRB: Volume 10, Environmental Design and Management, HA, Section 0, Part 3: Landscape Elements

Inclusive Design for Getting Outdoors (I'DGO):

www.idgo.ac.uk

Institution of Lighting Professionals:

All lighting on the TLRN should meet the requirements of industry-recognised codes of best and/or safe practice such as those recommended by the Institution of Lighting Professionals' Technical Reports and Guidance Notes including but not exclusively: Guidance Notes for the Reduction of Obtrusive Light

Bats and Lighting in the UK

Code of Practice for Electrical Safety in Highway Electrical Operations

Code of Practice for Variable Lighting Levels for Highways

Guidance Notes for the Reduction of Obtrusive Light GN01, 2011

Managing a Vital Asset: Lighting Supports

International Commission on Illumination:

CIE 115: Lighting of Roads for Motor and Pedestrian Traffic, 2010

Joint Mobility Unit:

Sign Design Guide, 2000

Legislation:

Climate Change Act 2008

Construction Design and Management Regulations 2007

Greater London Authority Act 1999

Health and Safety at Work Act 1974

Highway Authorities, Highways Act 1980

Guidance on the application of powers under Section 115, Highways Act 1980

Highways Act 1980, Section 132

Highways (Road Humps) Regulations 1999

London Local Authorities and Transport for London Act 2003

New Roads and Streetworks Act 1991

Equality Act 2010

Section 63 of the Road Traffic Regulation Act 1984 as amended by the Transport Act 2000 (Section 75)

Section 64, London Passenger Transport Act 1937

Section 32 or 45 of the Road Traffic Regulation Act 1984

Section 104 of the London Passenger Transport Act 1934

Town and Country Planning Act 1990 and The Town and Country Planning (Control of Advertisements) (England) Regulations 2007

The Electricity at Work Regulations 1989

Traffic Calming Act 1992

Traffic Signs Regulations and General Directions (TSRGD)

London Transport Users Committee:

Where am I? Street name signs in London, 2003

London Tree Officers Association:

Surface materials around trees in hard landscapes

Sustainable Water Management: Trees are part of the solution

National Joint Utilities Group:

NJUG Guidelines for the Planning, Installation and Maintenance of Utility Apparatus in Proximity to Trees, 2007

NJUG Guidelines on the Positioning and Colour Coding of Underground Utilities' Apparatus, 2007

Construction Industry Research and Information Association (CIRIA):

The SuDS Manual (C697)

Motorcycle Action Group:

A Guide to the Design and Provision of Secure Parking for Motorcycles, 2002

Office of Rail Regulation:

Guidance on Tramways: Railway Safety Publication 2

Sewers for Adoption:

(7th edition)

Susdrain:

(www.susdrain.org/)

Trees and Design Action Group:

Trees in Hard Landscapes: A Guide for Delivery, 2014

Transport Research Laboratory (TRL):

CSS SL1 – Review of the class and quality of street lighting, 2008

Footways and cycle route design, construction and maintenance guide

New York City, Department of Transportation:

Street Design Manual, 2013

Infrastructure Commission:

World class infrastructure for a world city, 2010

University College London:

Effective Kerb Heights for Blind and Partially Sighted People, Accessibility Research Group, UCL, 2009

UK Roads Liaison Group:

Well-maintained Highways – Code of Practice for Highway Maintenance Management, 2013

WRc Group (Water Research Centre)

Sewers for Adoption (7th edition), 2013

15.2 List of revisions

Revision number	Content	Date	Author	Reviewed by	Approved by
2016 Revision 1	Text and content corrections throughout Update to 2.4 Street Types for London Update to tramline and ladder paving policy on page 139	January 2016	Shannon Rice, Streetscape Manager	Matthew Wilson, Highways Manager – Sponsor	Dana Skelley, Director of Asset Management
2017 Revision 1	Text and content corrections throughout Update to Part A – A vision for London's Streets Update to seating/bench policy Update to vehicle crossovers	May 2017	Shannon Rice, Streetscape Manager	Matthew Wilson, Highways Manager – Sponsor	Dana Skelley, Director of Asset Management
2019 Revision 1	Text and content corrections throughout Update to 10.5 Electric vehicle charging points on page 188	March 2019	Jon Hodges – Streetscape Design Manager	Martin McMahon – Asset Management Strategy Lead	Garry Sterritt – Head of Asset Investment


20

Transport for London

Invitation to Quote

Electric Vehicle Infrastructure Delivery (EVID)
Tranche 2, Batch 1

Volume 2

Appendix G

TfL management system

COMMERCIAL IN CONFIDENCE

TfL Restricted

Procedure

PR1504 A1 Highways Technical Assurance Process

Formerly SQA-1900

Contents

1 Purpose 2
2 Scope 2
3 Background 2
3.1 Statutory Position 2
3.2 The Technical Assurance Authority 2
4 The Highways Technical Assurance Process 3
4.1 General Description 3
4.2 Relevant Documents 4
4.3 Procedure Flow 6
5 Procedure Description 7
6 Relevant Documentation 9
7 Person accountable for this document 9
8 Abbreviations 10
9 References 10
10 Document history 10

MAYOR OF LONDON
Transport for London

1 Purpose

This document sets out the Highways Technical Assurance (HTA) procedure for schemes that affect any aspect of the highway for which TfL is the Highway Authority.

2 Scope

This procedure applies to the highway for which TfL is the Highway Authority.

This procedure must be followed by anyone wishing to add or modify highway assets within TfL Highways Boundary.

3 Background

3.1 Statutory Position

The Highways Act 1980 imposes a number of duties on highway authorities, primarily the duty to maintain under Section 41 and the duty to assert and protect public rights to enjoyment of the highway under Section 130.

As per Section 58 of the Highways Act, to safeguard it against litigation, a highway authority may not simply rely on the reputation and competence of a third party, unless it has itself taken sufficient care to ensure that the services being provided are to the appropriate standards.

3.2 The Technical Assurance Authority

The Highways team within TfL Engineering is the Technical Assurance Authority (TAA) within 'TfL Engineering and Asset Strategy' (E& AS) for highways assets on behalf of Asset Operations (AO). AO within the Network Management and Resilience Directorate is the Highway Authority and discharges all duties and functions of the Highways Act 1980 on behalf of TfL, and the TAA represents AO in many of these functions .TAA also represents the interests of the Overseeing Organisation[1] for the Transport for London Road Network (TLRN) and is responsible for assessing and granting any departures from Design Manual for Roads & Bridges (DMRB) standards (where applicable).

The Highways team is able to call on extensive knowledge in highway design and construction, highway standards, highway legislation, and traffic regulations.

The Highways team can provide technical advice, product and material approval, value engineering, risk identification advice and design services. Requests for advice should be sent to Highways-TAA@tfl.gov.uk, and typically, be accompanied by a WBS code. It remains the duty of the Promotor of a given project to ensure compliance with all legislation.

[1] The Overseeing Organisation in this case is Transport for London.

4 The Highways Technical Assurance Process

4.1 General Description

The objectives of HTA is to give increased assurance that any new or amended highway assets is in accordance with relevant legislation; comply with British and European standards, as well as asset specific guidance; are economic to build and maintain; and do not introduce any unnecessary risk to the Highway Authority.

HTA applies to all proposals within or near to the TfL Highway Authority boundary. It applies to all forms of construction including renewals, enhancements and decommissioning of highway assets, with the exclusion of routine maintenance activities. HTA is independent of, and compliments, Structures Technical Approval.

Notwithstanding the series restrictions[2] in SHW, HTA will consider all aspects of the proposed design that affect the buildability[3], legality, operability, and maintainability of all highway assets as categorised in the Specification for Highways Works (SHW) and within the London Highway Maintenance and Projects Framework (HMPF) and the Surface Transport Infrastructure Construction Framework (STIC). Designs will be assessed against any relevant standards and specifications, including the Streets Toolkit. HTA does not in any way modify or reduce the contractual and statutory responsibilities of any party for the work carried out, the legal responsibilities of professional engineers, or confer any other approval of the proposals. The 'Assurance' of HTA is an agreement on behalf of the asset owner to alter the highway assets, and does not absolve the Promotor from obtaining any other approval required to work on the TfL highway (e.g. Traffic Management Act Notifications (TMAN), Permits, legal agreements etc).

It is mandatory for all proposals to be submitted and obtain Technical Assurance at the end of Pathway stage 4 (Detailed Design) prior to the scheme commencing works on site. HTA can be considered to have been granted upon receipt of a signed **Detailed Design – Approval Certificate**. Guidance from the HTA team should be sought for any changes to the design through the Build phase as a resubmission may be required for an additional Approval Certificate.

It is strongly recommended that a scheme is submitted at the end of Pathway stages 2 and 3 (Option Selection and Concept Design) to highlight any potential issues early and to de-risk future stages. Design programmes should allow sufficient time for this process and subsequent revisions to be undertaken. When an Option Selection/Concept submission is suitably developed, an **Approval in Principle** (AIP) will be issued confirming that the Highways team believe the design is in a sufficient position to move to the next stage. If the AIP is not issued, the Highways Team do not believe the design should progress, but the Promotor can choose to do so anyway at risk.

[2] Note that series 1600 – 2500, and series 5000 of the SHW are covered by colleagues in Engineering & AS's 'Surface and Highway Structures' team, so are excluded from HTA.
[3] Buildability in a HTA sense differs from the Construction Management Team's buildability reviews in that Construction Management Team generally consider alternative options to reduce cost and construction risk, whereas HTA generally considers ancillary risk and avoidance of unapproved design alterations.

The standard response time from submission of Designs to the Highways TAA team to return of HTA feedback is 28 calendar days for all types of submission. For smaller schemes or for earlier design stages, the actual response time can be, and frequently is significantly less. It should be noted that multiple iterations and submissions may be required. For very large and/or complex schemes, a different response time or submission regime may need to be agreed in advance. For advice, please contact Highways-TAA@tfl.gov.uk.

Should a dispute arise between the scheme Promotor and the Technical Assurer (TA), the initial escalation point should be to the Portfolio Delivery Engineering Lead (PDEL), the PDEL will discuss concerns with the Highways Principal Engineer and the relevant Senior Portfolio Sponsor for Investment Delivery Planning (IDP) (or Scheme Promotor). If resolution is still unable to be achieved, the final escalation point for a decision is the Head of Engineering for Roads, Streets and Places, the Head of Profession for Highways and Traffic and the Head of IDP (or head of the Scheme Promotor).

A step by step guide of the overall process is given in Section 5.

4.2 Relevant Documents

The required documents to obtain HTA for the completion of each stage will vary widely depending on the size, scope, and complexity of the scheme. The list of documents described below is therefore not exhaustive, but gives an indication of typical requirements at the end of each stage. Each document will not always be required for every scheme – advice from Highways-TAA@tfl.gov.uk should be sought if the Promotor is unsure (* indicates a required document, {P} refers to a document from the Pathway suite of products).

Option Selection (Pathway Stage 2)

- General Arrangement drawing*
- F7185 Highways Approval Document (HAD)*
- Vehicle Tracking of appropriate vehicles
- Operational Concept {P}
- Maintenance Concept {P}
- Stage 1 Road Safety Audit report if applicable

Concept (Pathway Stage 3)

- HAD*
- Updated General Arrangement drawing*
- Concept drawings for each SHW series (can be combined into one or more drawings)
- Updated Stage 1 Road Safety Audit report
- Cross-sections and Longitudinal section where alignment/level change is proposed
- AIP from Option Selection (HAD)

- Updated Vehicle Tracking
- Operational Readiness Plan {P}
- Maintenance Readiness Plan {P}
- Surveys and Investigation reports (e.g. California Bearing Ratio (CBR), Cores, Ground Penetrating Radar (GPR) {all types}, Drainage, Lighting, Utilities, Arboriculture, Pavement Design, Duct survey, etc, as applicable)
- Design assumptions and calculations
- F7283 Departures from Standard
- Asset Ownership details (electrical supplies, utility covers, Highway boundary etc)
- For construction, resurfacing, or widening of pavement/footway layers, the layers and depths of construction have been determined

Detailed (Pathway Stage 4)

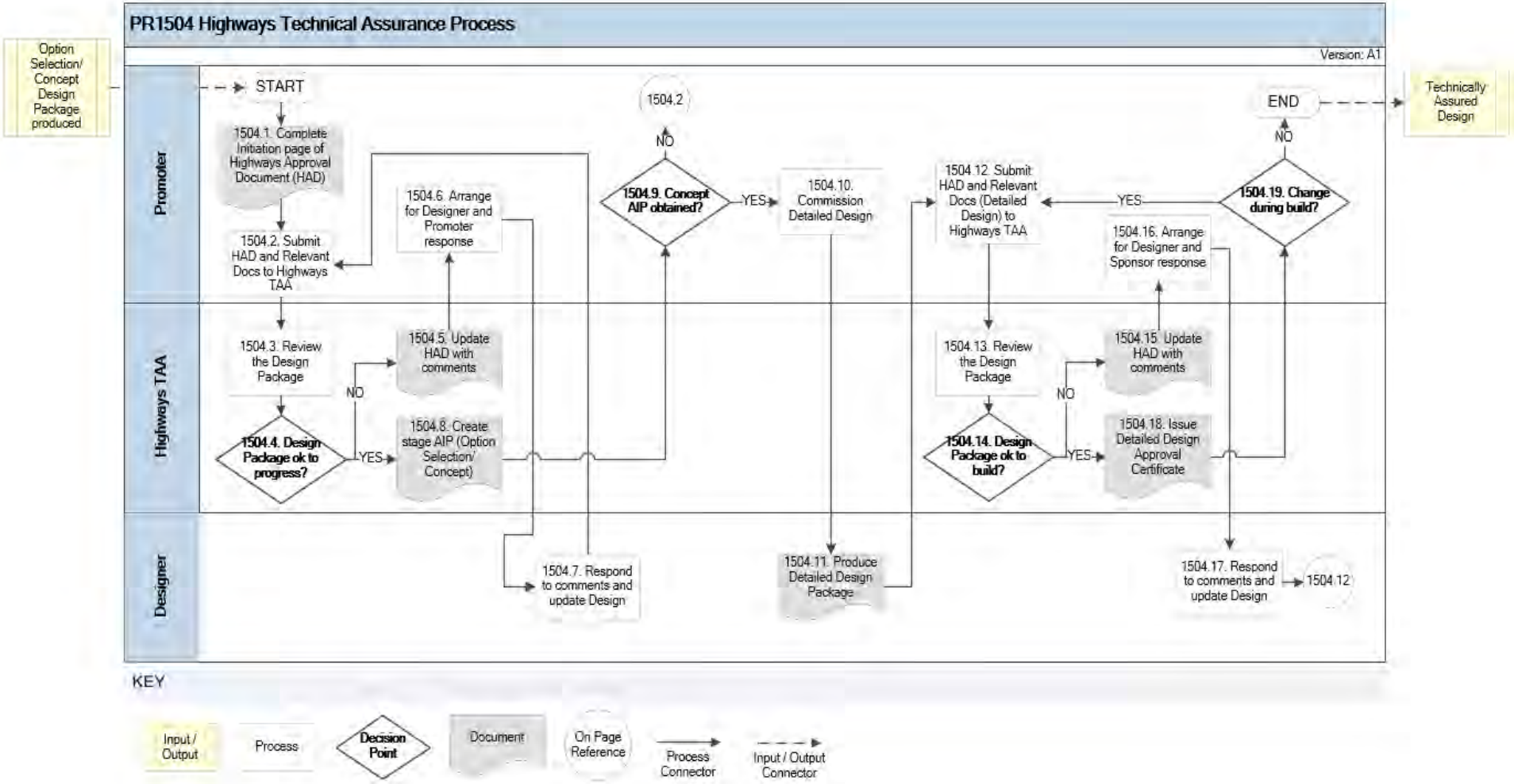
- HAD*
- Detailed Design drawings for each SHW series (can be combined into one or more drawings)*
- AIP from Concept (HAD) where applicable *
- Stage 1/2 Road Safety Audit with designer response where applicable
- Operational Readiness Plan {P}
- Maintenance Readiness Plan {P}
- Design calculations (pavement, drainage, lighting etc)
- Departures from Standard AIP from Concept
- Any appropriate information not provided at Concept (Stage 3)

Build (Pathway Stage 5)

- Similar documents to Detailed Design when a change is required to the design during build.

MAYOR OF LONDON
Transport for London

4.3 Procedure Flow



5 Procedure Description

Inputs:

- Option Selection/Concept Design Package produced for the scheme.

1504.1. Complete Scheme Initiation page of Highways Approval Document (HAD)

The Promoter completes the first tab of the F7185 Highways Approval Document, which provides basic scheme information to the TAA. Note that the Promoter can either be the Sponsor or the Project Manager.

1504.2. Submit HAD and Relevant Documents to Highways TAA

The Promoter submits the HAD and Relevant Documents (refer to section 3.2 for a description of the relevant documents at each stage) to the Highways-TAA@tfl.gov.uk inbox. Note that the Promotor would typically be the Sponsor, however they may choose to delegate this task to the Project Manager.

1504.3. Review the Design Package

The allocated Highway TA will review the submitted package in line with section 3.1 and seek input from Arboriculture and Landscape (A&L) team, Electrical and Mechanical (E&M) team, Pumps and Drainage team (P&D) or any other discipline specific subject matter expert (SME) where applicable.

1504.4. Design Package ok to progress?

The TA makes an assessment on whether the Package is suitable to progress to the next design stage.

If the answer is NO, please refer to step **1504.5.**

If the answer is YES, please refer to step **1504.8.**

1504.5. Update HAD with comments

The TA provides itemised commentary on the second tab of the HAD highlighting issues that require resolution prior to making a positive recommendation to proceed, and returns the HAD to the Promoter.

1504.6. Arrange for Designer and Promoter response

The Promoter arranges for the Designer to provide a response to each of the issues raised by the TA in the relevant column of the HAD. The Promoter should also provide commentary on all items. It is often beneficial at this stage for the Promoter to arrange a meeting with the TA and the Designer to discuss each of the issues in person.

1504.7. Respond to comments and update Design

The Designer completes their response to each of the issues in the HAD, and updates the Design Package where appropriate. The Promoter should review each response prior to resubmitting by returning to step 1504.2. Note that it is essential that the Promoter reviews and responds to each comment as not all are specifically design related.

1504.8. Create stage AIP (Option Selection/Concept)

Once the Design Package is considered sufficiently developed to progress to the next design stage, the TA should produce either an "Option Selection Approval In Principle" (at the end of Option Selection Design), or a "Concept Approval In Principle" (at the end of Concept Design). This certifies that Highways TAA is satisfied that the Stage Gate can be signed

1504.9. Concept AIP obtained?

If the AIP issued in step 1504.8 is an Option Selection AIP, return to steps 1504.2 for the Concept Design package. If the AIP issued in step 1504.8 is a Concept AIP, proceed to step 1504.10.

If the answer is NO, please return to step **1504.2.**

If the answer is YES, please progress to step **1504.10.**

1504.10. Commission Detailed Design

The Promoter requests a Designer to produce a Detailed Design Package for the scheme.

1504.11. Produce Detailed Design Package

The Designer produces the Detailed Design Package using the information provided from the Concept AIP. Concurrently, the Promoter should be producing the relevant Pathway documentation.

1504.12. Submit HAD and Relevant Documents (Detailed Design) to Highways TAA

Once the Detailed Design Package is complete, the Promoter submits the HAD and Relevant Documents (refer to Section 3.2) to the Highways-TAA@tfl.gov.uk inbox.

1504.13. Review the Design Package

The allocated TA will review the submitted package in line with section 3.1.

1504.14. Design Package acceptable to build?

The Highway Technical Approvals team member makes an assessment on whether the Package is suitable to be approved for Build.

If the answer is NO, please return to step **1504.15.**

If the answer is YES, please progress to step **1504.18.**

1504.15. Update HAD with comments

The TA provides itemised commentary on the second tab of the HAD highlighting issues that require resolution prior to approving the Design for build, and returns the HAD to the Promoter.

1504.16. Arrange for Designer and Promoter response

The Promoter requests the Designer to provide a response to each of the issues raised by the TA in the relevant column of the HAD. The Promoter should also provide commentary on all items. It is often beneficial at this stage for the Promoter to arrange a meeting with the TA and Designer to discuss each of the issues in person.

1504.17. Respond to comments and update Design

The Designer completes their response to each of the issues in the HAD, and updates the Design Package where appropriate. The Promoter should review each response prior to resubmitting at step 1504.12. Note that it is essential that the Promoter reviews and responds to each comment as not all are specifically design related.

1504.18. Issue Detailed Design Approval Certificate

Once the Design Package is sufficient to be approved, the TA should issue a "Detailed Design – Approval Certificate". This certifies that Highways TAA has been obtained, so the TA is content for the scheme to progress to build. It does not accept any design liability on behalf of TfL.

1504.19. Change during build?

Upon any form of design change becoming necessary, the appointed HTA should be consulted to determine whether a full resubmission is required, or a verbal/email confirmation is sufficient. Should a substantial change be required to the design, a resubmission of the Relevant Documents may be required as determined by the TA. It is recognised that changes during delivery are often crucial in terms of timescales, so priority will be given to assessing these over schemes in earlier stages of design.

Outputs:

- Technically Assured Design

6 Relevant Documentation

- Departures from Standard
- F7185 Highways Approval Document
- HMPF/ STIC Technical Specification
- Pathway
- Specification for Highways Works
- Streets Toolkit
- The Highways Act 1980

7 Person accountable for this document

Name	Job title
Ryan Cooper	Principal Engineering Leader – Highways & Traffic (Interim Head of Profession H&T)

8 Abbreviations

Abbreviation	Meaning
AIP	Approval in Principle
AS	Asset Strategy
GPR	Ground Penetrating Radar
HAD	Highways Approval Document
HTA	Highway Technical Assurance
IDP	Investment Delivery Planning
HMPF	Highways Maintenance and Projects Framework
SHW	Specification for Highways Works
STIC	Surface Transport Infrastructure Construction Framework
TA	Technical Assurer
TAA	Technical Assurance Authority
TfL	Transport for London
TLRN	Transport for London Road Network
TMAN	Traffic Management Act Notifications

9 References

Document no.	Title or URL
F7185	Highways Approval Document (HAD)
F7283	Departures from Standard

10 Document history

Issue no.	Date	Changes	Author
1.1	18/09/2015	First Issue	Highways Technical Approvals Engineer (Lixi Pan)
2.0	16/12/2016	Full rewrite following 12 months of operation v2	Highways Technical Approvals Manager (Ryan Cooper)
3.0	17/07/2023	Update following business transformation (draft)	Senior Engineering Leader (Lixi Pan)
A1	December 2023	SQA-1900 reformatted and updated to new TMS document format as part of change request CR-18541	Lukash Manandhar Principal Engineer

Transport for London

Invitation to Quote

Electric Vehicle Infrastructure Delivery (EVID)
Tranche 2, Batch 1

Volume 2

Appendix H

SQA 0170 Road safety audit

COMMERCIAL IN CONFIDENCE

TfL Restricted

Transport for London
Surface Transport

Management System Document – Procedure

Road Safety Audit

Document reference: SQA-0170 - issue: 1

Uncontrolled when printed – may contain out of date information.

Contents

1 Purpose 3
2 Background / Scope 3
3 Procedure Flow 1 9
Where an Audit Team internal to TfL is to be appointed 9
4 Procedure Description 1 10
Where an Audit Team internal to TfL is to be appointed: 10
5 Procedure Flow 2 16
Where an Audit Team external to TfL is to be appointed 16
6 Procedure Description 2 17
Where an Audit Team external to TfL is to be appointed 17
7 Relevant Documentation 25
8 Document Control 25

1 Purpose

This document describes the Procedure that must be followed when carrying out Road Safety Audits (RSAs) on the Transport for London Road Network (TLRN), its assets and locations managed or maintained by TfL (such as Station forecourts and footways). It should be noted that TfL is also Traffic Authority for roads in proximity to the TLRN and this Procedure must also be followed when undertaking RSAs in these locations.

This procedure will also be followed when TfL undertakes RSAs on non-TLRN schemes (e.g. Borough schemes), with the exception of Trunk Road locations, which must be carried out in accordance with the latest Road Safety Audit Standards in the Design Manual for Roads and Bridges (DMRB), currently HD19/15. This Procedure is commended to all others involved in commissioning and undertaking RSAs on non-TLRN schemes in London.

An RSA considers the road safety implications of all measures, their impact on the network under all anticipated operating conditions, and their road safety implications on all types of road user. Fundamental to the principle of an RSA, is ensuring that due consideration is given to the effects of any proposal on all road users and especially all vulnerable user groups, generally regarded to include the very young, the elderly, people with a disability, pedestrians, cyclists and riders of powered two wheeled vehicles. In some cases, the specific needs of equestrians will also need to be considered.

This is in accordance with the following:

- Mayor's Transport Strategy, Chapter 5, Part 3
- Safe Streets for London – The Road Safety Action Plan for London 2020

2 Background / Scope

This Procedure is **mandatory** and must be followed without exception to identify when a Road Safety Audit is required and set the standard and process for carrying out RSAs.

The **mandatory** workflow process for Road Safety Audits undertaken internally by Transport for London is shown in Section 3.

The **mandatory** workflow process for Road Safety Audits undertaken by all other parties, including those employed under TfL Contracts, developers and third parties is shown in Section 5.

This Procedure will be subject to frequent revision to ensure it reflects current best practice. Users of this Procedure should ensure they are using the most recent

version, a copy of which will be available on TfL's website. Notifications of updates will be sent to registered interested parties. If you wish to be included on this distribution list please notify TfLSafetyAudit@tfl.gov.uk.

This Procedure shall apply to:

- All measures proposed on the TLRN, its assets and locations managed and maintained by TfL (including where TfL is the Traffic Authority) that involve permanent changes to the highway;
- Works carried out under agreement with TfL resulting from developments alongside or affecting the TLRN;
- Temporary Traffic Management Schemes lasting longer than 3 months or where it is anticipated that the proposals are likely to have a significant impact on the highway network or road safety concerns have been identified. Phased traffic management schemes where each phase is less than 3 months, but the combined total of all phases exceeds 3 months, must be audited; and,
- Like for like replacements where there is a known collision risk. For example, the replacement of a non-passively safe traffic sign in the same location where it has been previously struck by errant road users on numerous occasions.

The RSA will not include:

- A technical check to ensure compliance to standards.
- Non-safety related issues (although discretion is given to Auditors to provide comment on these issues separately within the standard Road Safety Audit reporting method).
- Issues relating to the stability of any structure, or the structural integrity of any proposed element or method of construction.
- Construction and maintenance issues as covered by current Construction Design and Management (CDM) Regulations. The RSA covers only the future operational road safety of the scheme. Overseeing Organisation Project Clients, Sponsors and Directors should make themselves aware of current Health & Safety legislation and consider the implications of their instructions to Design Teams and Road Safety Audit Teams in terms of Health & Safety.
- Traffic signal design / safety checks which are covered by separate TfL Procedures. These exist to ensure that all aspects of safety are considered during the design stage so that the traffic signal scheme can be implemented, operated, maintained and decommissioned in a safe manner and the design accords with the requirements of CDM. Those

design / safety checks do not replace the necessity for an RSA in accordance with this Procedure.

- A definitive judgement on which option is preferable if separate options are submitted for audit. The RSA Team will assess each option individually and make recommendations accordingly. The decision on which option to develop will remain entirely with the Client Organisation.

The RSA is not an opportunity to:

- Query why other measures are not being proposed;
- Comment on the operational characteristics of the proposals where there are no adverse safety implications; or,
- Suggest alterations or additions to the proposals which are not as a result of a specified safety concern.

No part of an RSA report should be regarded as a direct instruction to include, remove or amend any scheme element. Responsibility for designing the scheme lies with the Design Organisation and as such the Audit Team will accept no design responsibility for any changes made to a scheme following the completion of an RSA Report.

All pre-construction RSAs have a maximum shelf life of two years and should be repeated if the next stage in the scheme's development has not begun within two years following completion of the RSA. This is to ensure that the schemes interface with the current highway network and its current usage is assessed. Similarly, RSAs should be repeated if any element of a scheme is significantly changed, or the highway layout is substantially altered, subsequent to an RSA having been undertaken.

Road Safety Audit Stages and Associated Milestones

Road Safety Audit is not a single Procedure undertaken once for each scheme. An RSA and its subsequent actions shall be undertaken following completion of specific stages of a scheme's development. The scheme design must be sufficiently progressed such that all significant features are clearly shown to a degree that would enable it to progressed to the next stage of the design or proceed to construction accordingly. These stages are:

a) Stage 1: Completion of Preliminary Design / Conceptual Design

b) Stage 2: Completion of Detailed Design

As a guide, the following information should be provided as appropriate:

- General arrangement details (fully dimensioned)
- Site clearance details

- Traffic signs and road markings
- Drainage alterations
- Street lighting alterations
- Traffic signal details and traffic signal staging alterations
- Carriageway and footway level alterations
- Swept path analysis
- Surfacing and material details / specifications

c) Stage 3: Completion of Construction

To be undertaken as soon as practicable after the works are complete. The Client may also deem it prudent to carry out an RSA on a scheme prior to full completion, so that any significant issues arising can be addressed with immediacy. Where an RSA is carried out before a scheme is complete, a further RSA will also be carried out as soon as practicable upon completion.

Under normal circumstances, a Stage 3 RSA should be completed as soon as reasonably practicable, but within 3 months following completion of a scheme. A scheme is regarded to be complete and operational from the date construction ceases on site, the location is open to the general public and all traffic management has been removed. Consideration should be given to allow a period post construction for the modified layout to bed-in.

d) Stage 4: Monitoring

Stage 4 RSAs are not routinely undertaken on TfL schemes. TfL monitors the performance of highway engineering schemes through the Traffic Accident Diary System (TADS). Where TADS identifies an emerging collision problem, the Client should commission a Stage 4 RSA. Stage 4 RSAs are purposely not shown on the workflow in Section 3 and Section 5.

At stage 4, the collision records are analysed in detail to identify the locations at which personal injury collisions have occurred, where collisions appear to arise from similar causes or show common factors and how the scheme may have affected collision patterns and rates. Comparisons with control data such as Collision Risk in Greater London, will also be undertaken to identify collision patterns and trends. The Stage 4 Audit report will comprise of an analysis of the collision data to identify the impact of problems and recommendations at previous Audit stages; details of other notable events that have occurred since construction where this is known to the Audit Team; identify any road safety problems linked to the scheme and indicated by the data analysis and observations during any site visits undertaken. The reports should make recommendations for remedial action.

If a pattern of collisions are identified during the hours of darkness, it may be prudent to consider a night time site visit supplementary to the daytime visit.

- A Stage 4a RSA will be prepared using 12 months of collision data from the first full month after the scheme became operational and 36 full months of collision data from prior to the commencement of construction works.

- A Stage 4b RSA is prepared using 36 months of collision data from the first full month after the scheme became operational and 36 full months of collision data prior to the commencement of construction works. The Client Organisation must decide if a Stage 4b RSA needs to be prepared. This decision may be led by the results of the Stage 4a report, the scale of the changes instigated by the original scheme, TADS outputs and any issues highlighted since the completion of the scheme.

e) Supplementary Road Safety Audit stages

In addition to the defined stages specified above, it may at times be beneficial to conduct Interim or combined Stage 1 & 2 audits as follows:

- For large, complex schemes, particularly with accelerated programmes, the Client Organisation may consider at any time during the design or construction stages, that it is appropriate to undertake an Interim RSA. Interim RSAs shall be carried out following the same procedure as for the formal Audit stages, which must still be undertaken in full. Where applicable, the Audit Team, Client and Designer can meet if considered necessary to enable the Design Organisation to explain their designs and the Audit Team to explain any identified problems and recommendations.

- Combined Stage 1 & 2 RSAs can be carried out on the overall design of smaller and simpler schemes. Combined Stage 1 & 2 RSAs may have the disadvantage of identifying potential safety issues late in a scheme's development when corrective action may be more difficult. It is envisaged that schemes such as road marking alterations, traffic signing schemes and small footway modifications would fall under this category. Stage 1 and Stage 2 Road Safety Audits must not be combined as purely a cost and/or programme saving measure.

In exceptional circumstances, such as when auditing unique and complicated schemes to tight deadlines, it is permissible to deviate away from this Procedure to suit the specific scheme circumstances. The decision to change the way in which Audits are undertaken can only be made by TfL's Road Safety Audit Manager without exception. In all cases, written approval must be sought and the reasons for modifying the Road Safety Audit Procedure must be stated within the Audit report.

f) Pre Stage 1 Road Safety Audit comments

For large complicated schemes or for schemes with multiple possible options, it may be beneficial to enlist the help of Road Safety Audit to provide advice on the potential road safety implications of the proposals to assist optioneering. Providing this advice does not preclude the necessity to undertake a formal Stage 1 Road Safety Audit.

In providing advice the RSA team will not form part of the project team and will remain impartial. Providing pre-Stage 1 advice does not prevent the same Auditors from undertaking the formal Audit of the proposals.

Retention of Records

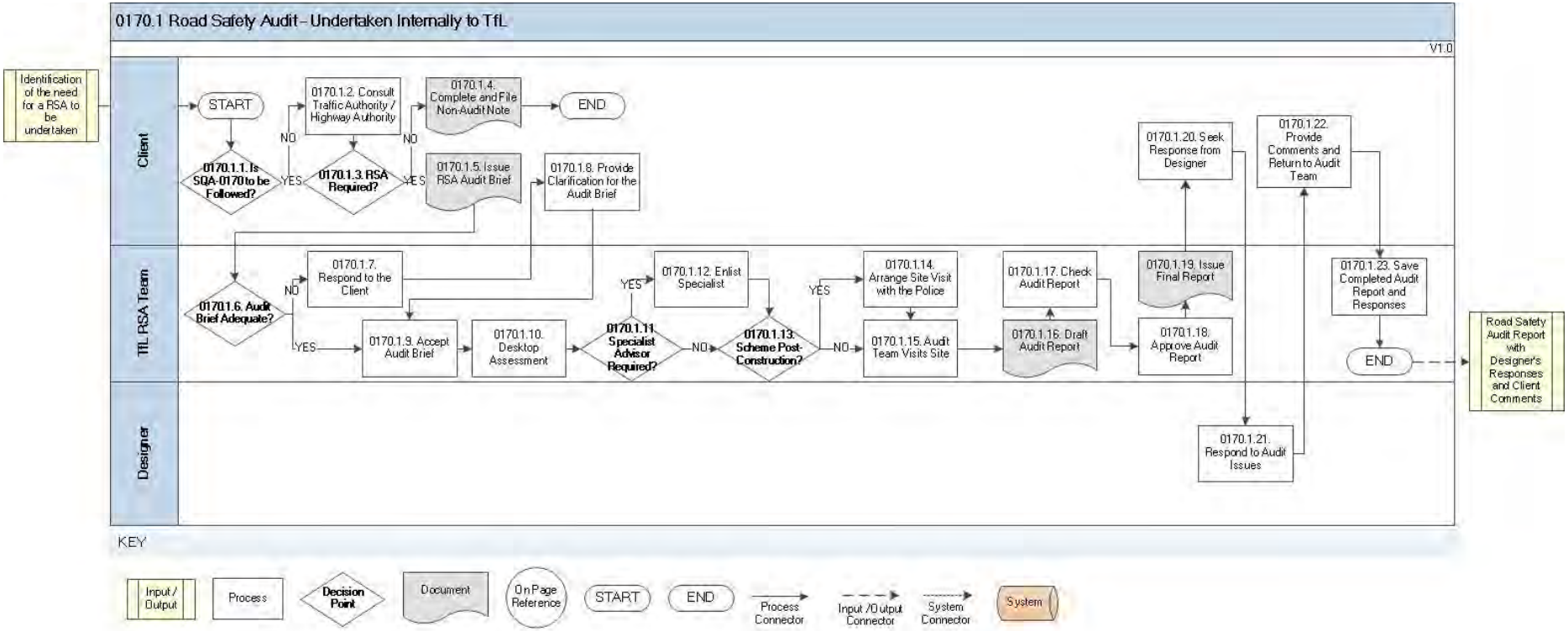
In accordance with TfL's document retention Policy for Road Safety Audit reports and related information, these records must be retained for a period of 21 years from the date the report is issued.

It is the responsibility of any Client Organisation's external to TfL to ensure all Road Safety Audits are retained in accordance with their own Policy.

Filing and retention arrangements for Road Safety Audits must pay due regard to complying with the Freedom of Information Act.

3 Procedure Flow 1

Where an Audit Team internal to TfL is to be appointed



A Visio version is available here: LINK.

4 Procedure Description 1

Where an Audit Team internal to TfL is to be appointed:

Inputs:

- Identification of the need for a Road Safety Audit to be undertaken.

0170.1.1. Is SQA-0170 to be followed?

The Client should identify the ownership of the road network / asset. If the proposal is located on or affects the TfL road network, land or assets, or if a non-TLRN road is to be audited by the TfL RSA Team, SQA-0170 must be followed.

This requirement specifically excludes the scenario where a Road Safety Audit is required on the Highways England road network. In this scenario, the requirements of the Design Manual for Roads and Bridges HD19 must be followed.

If the answer is YES, please refer to step **0170.1.3**.

If the answer is NO, please refer to step **0170.1.2**.

0170.1.2. Consults Traffic Authority and/or Highway Authority

The Client liaises with the Traffic Authority and/or Highway Authority to ascertain the requirements for Road Safety Audit.

0170.1.3. RSA Required?

Does the scheme constitute a change to the highway as outlined in Section 2 of this Procedure and therefore requires an RSA to be carried out?

If the answer is YES, please refer to step **0170.1.5**.

If the answer is NO, please refer to step **0170.1.4**.

0170.1.4. Client Completes and Files Non-Audit Note

If the Client deems that an RSA is not required for the scheme, they must complete a Non-Audit Note stating the reasons that an RSA will not be undertaken and retain the document within the project file.

0170.1.5. Client Completes and Sends RSA Audit Brief to TfL RSA Team

The Client compiles the Audit Brief consisting of a completed Audit Brief Checklist and any drawings and further supporting information necessary to assist the Audit Team. Details of what drawings and further information may be required can be discussed with TfL's RSA Team, but as an absolute minimum the Audit Brief Checklist and a General Arrangement drawing should be provided.

0170.1.6. Audit Brief Adequate?

TfL RSA Team assesses if the Audit Brief has the necessary information required to undertake the Audit.

If the answer is YES, please refer to step **0170.1.9**.

If the answer is NO, please refer to step **0170.1.7**.

0170.1.7. Respond to the Client

TfL RSA Team responds to the Client indicating why the Audit Brief has not been accepted or seeks clarification.

0170.1.8. Provide Clarification for Audit Brief

The Client provides the TfL RSA Team with clarification or additional drawings and information as required.

0170.1.9. Accept Audit Brief

The Audit is added to the central repository database, prioritised accordingly and the internal Audit Team selected by the Road Safety Audit Manager.

The Audit Team will comprise of at least two persons, one of which will lead the Audit (Team Leader), the other (Team Member) will provide technical expertise to assist the Audit Team Leader.

The educational and experience requirements of the Audit Team are at the discretion of TfL's Road Safety Audit Manager. As a general principle, educational and experience requirements for internal Road Safety Auditors will exceed the mandatory requirements for Auditors external to TfL.

On occasions an individual with the appropriate training, skills and experience may accompany the RSA Team as an Observer in order for them to gain experience of the Audit process and they are actively encouraged to contribute. As a minimum an Observer must have undertaken a 10-day formally structured and recognised Collision Investigation or Road Safety Engineering course and have a minimum of 1 year's Collision Investigation or Road Safety Engineering experience.

0170.1.10. Desktop Assessment

The appointed Audit Team collects the latest collision data and carries out analysis to ascertain any underlying collision patterns. This data is to be used to determine current safety concerns which may not be discernible from the site visit alone and builds a greater appreciation of the future operation of the proposals. A desktop assessment of the drawings and information supplied is carried out prior to visiting the site.

0170.1.11. Specialist Advisor Required?

If there are any unusual or specialist measures to be audited, then the Audit Team Leader may elect to appoint an appropriate specialist to advise the RSA Team.

If the answer is YES, please refer to step **0170.1.12**.

If the answer is NO, please refer to step **0170.1.13**.

0170.1.12. Enlist Specialist

Audit Team identifies a Specialist Advisor and obtains their comments, advice and suggestions. It may be necessary to visit the site together.

The Police, Specialist Advisors and Observers do not form part of the formal Audit Team and are not required to be members of the Society of Road Safety Auditors (SoRSA) or meet the requirements of the formal Audit Team Members.

0170.1.13. Scheme Post-Construction?

The Audit Team identifies if the scheme has already been constructed and therefore requires a Police visit / comments and a night-time site visit.

If the answer is YES, please refer to step **0170.1.14**.

If the answer is NO, please refer to step **0170.1.15**.

0170.1.14. Arrange Site Visit with the Police

At Stage 3, the Team Leader shall invite representatives from the Police to accompany the Audit Team to offer their views for the Audit. Where it proves not possible to arrange a mutually convenient time, the Police will be invited to submit their views in writing. To expedite the Audit process, the Audit Team may visit the site and compile the Audit report in advance of the Police visit, at which time the Audit may be issued in draft.

At Stage 3 and in addition to the daylight site visit, all members of the Audit Team should visit the site of the scheme together during the hours of darkness to identify hazards particular to night-time operation. Seasonal variation will sometimes necessitate undertaking night-time site visits at a late hour. In such cases, the Team Leader may elect to defer the night time site visit, particularly if the personal safety of the Audit Team is considered to be an issue. When deferring the night-time site visit, the Audit report will be issued in draft form until such time as the night-time site visit is undertaken. Night time site visits may not be deferred for more than three months from the daytime site visit.

At the Team Leader’s discretion, and in consultation with the Client Organisation and TfL Road Safety Audit Manager, the site may not require a visit during the hours of darkness. In such instances the reasons for not visiting the site at night must be stated within the Audit report. It should be noted that choosing not to visit the site at night should be adopted only in exceptional circumstances.

0170.1.15. Audit Team Visits Site

At each stage of the Audit process, all members of the Audit Team must visit the site of the scheme together during daylight hours. The Audit Team must consider the measures from the perspective of all the road users that may be anticipated to use the scheme. Where appropriate, a combination of driving, walking and cycling through the scheme may be used to assist their evaluation and ensure that they have a comprehensive understanding and appreciation of the scheme. The Audit Team should also consider the effects of different weather conditions and site conditions that may affect the operation of the scheme.

Where the Audit Team identifies an immediate safety concern, they should notify the Client as soon as reasonably practicable. This is particularly important for problems identified during the Stage 3 RSA process.

The Audit Team Leader liaises with the Client, Police and Specialists Advisors as necessary in order to ensure the Audit report can be appropriately completed. It may be necessary to revisit the site.

0170.1.16. Draft Audit Report

The Audit Team compiles the Audit report at pre-construction, post-construction or Stage 4. The problems and recommendations in the Audit Report should be set out in a logical sequence. The use of headed sections and the details of those headed sections are at the Audit Team Leader's discretion. The Audit Team must avoid the use of superfluous headings for which no issues have been identified.

Road Safety issues that are beyond the scope of the RSA but that the Audit Team believes should be brought to the attention of the Client Organisation, may be included within Section 4 of the RSA report. These issues could include areas where repair or renewal may be required, operational concerns or existing poor provision. Such issues should be clearly identified as being beyond the scope of the RSA and should not be integrated into the main Problem and Recommendation section of the report.

Section 4 is not intended as an opportunity to provide a record of inspection of the existing site conditions. Only significant issues should be included as a large number of issues within this Section may remove focus from the genuine areas of concern. Existing issues and problems outside the geographical extents of the scheme should not normally be included within Section 4, unless they impact directly on the operation or delivery of the scheme.

0170.1.17. Check Audit Report

The draft Audit report shall be distributed amongst other members of the Audit Team to check and provide comments. Any necessary changes to the Audit report will be made, but the Audit Team Leader shall take responsibility for the content of the Audit report.

0170.1.18. Approve Audit Report

The amended draft Audit report will be read by the TfL's Road Safety Audit Manager or their delegated representative as appropriate, to ensure that the Audit report is understandable by those without a background in the field. The Audit Report approver will not instruct the Audit Team to modify the technical content within Road Safety Audit reports.

0170.1.19. Issue Final Report

The Audit Team Leader issues the Final Audit report to the Client and the Designer where appropriate.

0170.1.20. Seek Response from Designer

Where necessary, the Client sends the Audit report to the Designer and seeks their response to the Audit.

0170.1.21. Respond to Audit Issues

The Designer responds to each problem identified in the Road Safety Audit and this is recorded in the Designer's response areas of the Audit report. The response will contain details of how the problems identified in the Audit report will be resolved. Where the Designer disagrees with the problems or recommendations identified in the Audit report, or decides that the solutions recommended are not appropriate, the response justifies the alternative action to be taken. The Audit report is then signed off by the Designer and sent to the Client for comments.

It should be noted that the Designer must demonstrate due consideration of the problems raised when responding to the RSA report.

0170.1.22. Provide Comments and Return to Audit Team

It is the responsibility of the Client to review the RSA report and ensure that each problem identified is given due consideration by the Designer, adding comments in the relevant sections of the RSA report as appropriate.

The RSA report incorporating the Designer's and Client Organisation's comments is signed off by the Client Organisation and a copy is forwarded to the Audit Team Leader for information.

The Audit report is not an opportunity for the Client and the Designer to document their differences. Any disagreements relating to the progression of the proposals should be discussed and agreed separately. The agreed way forward should be documented within the Designer's response section. The Client Organisation is encouraged to use the Client section to provide background information to complement the Designer's decisions that may be beneficial to those reading the Audit report.

The Client Organisation should familiarise themselves with the requirements of CDM when issuing instructions to the Designer that could constitute a design decision.

With the agreement of TfL's Road Safety Audit Manager, alternative response / comment / sign-off roles and arrangements may be considered to suit local circumstances, but only with the approval of all parties involved.

The Client Organisation commissions the Design Organisation or others if applicable, in respect of changes required to the scheme arising from the Audit response. A scheme should be submitted for Audit again if significant changes are made to it as a result of an Audit.

The response sections of the Audit report must be completed and signatures added before the next stage in the scheme's development is begun.

0170.1.23. Save Completed Audit Report and Responses

The Audit Team Leader then saves the completed Audit report and responses within the central repository for their records. The Audit Team Leader ensures that all working documents supplied as part of the Audit Brief, including plans and maps are collated and retained. However, the record of Road Safety Audits is held by the Road Safety Audit Team for reference and should not be relied upon as a master record.

It is the responsibility of the Client Organisation to retain the master copy of the signed final Road Safety Audit Report incorporating the Road Safety Audit Response. Filing and retention arrangements for Road Safety Audits must pay due regard to complying with the Freedom of Information Act.

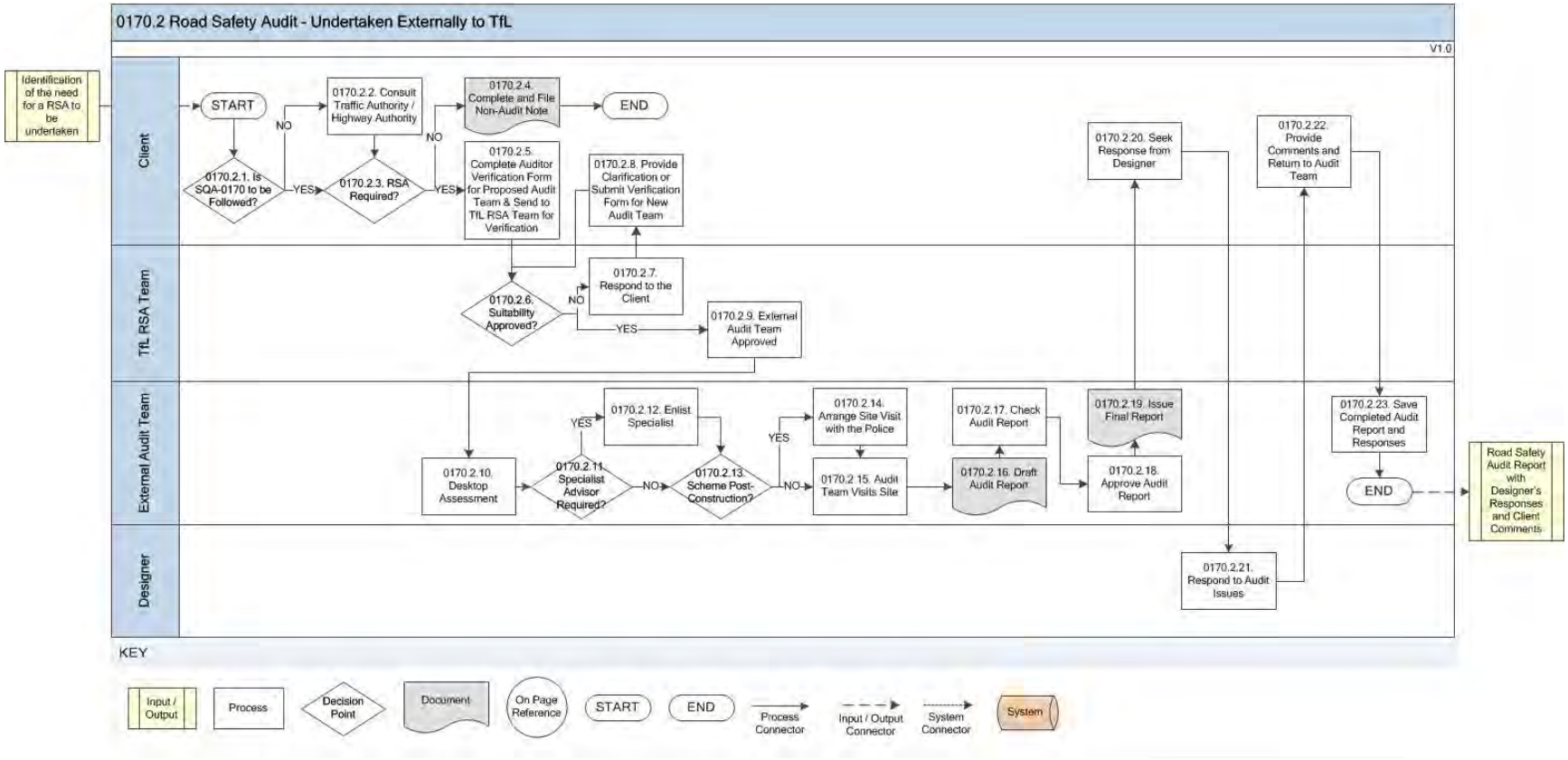
It is the responsibility of any Client Organisation's external to TfL to ensure all Road Safety Audits are retained in accordance with their own Policy.

Outputs:

- Road Safety Audit Report with Designer's Responses and Client Comments

5 Procedure Flow 2

Where an Audit Team external to TfL is to be appointed, including LoHAC contractors and private developers



A Visio version is available here: LINK.

6 Procedure Description 2

Where an Audit Team external to TfL is to be appointed, including LoHAC contractors and private developers

Inputs:

- Identification of the need for a Road Safety Audit to be undertaken.

0170.2.1. Is SQA-0170 to be followed?

The Client should identify the ownership of the road network / asset. If the proposals are located on or affect the TfL road network, land or assets, SQA-0170 must be followed.

If the answer is YES, please refer to step **0170.2.3**.

If the answer is NO, please refer to step **0170.2.2**.

0170.2.2. Consult Traffic Authority and/or Highway Authority

The Client liaises with the Traffic Authority and/or Highway Authority to ascertain the requirements for Road Safety Audit.

0170.2.3. RSA Required?

Does the scheme constitute a change to the highway as outlined in Section 2 of this Procedure and therefore requires an RSA to be carried out?

If the answer is YES, please refer to step **0170.2.5**.

If the answer is NO, please refer to step **0170.2.4**.

0170.2.4. Client Completes and Files Non-Audit Note

If the Client deems that an RSA is not required for the scheme, they shall complete a Non-Audit Note noting the reasons that an RSA will not be undertaken and retain the document within the project file.

0170.2.5. Complete Auditor Verification Form for Proposed Audit Team & Send to TfL RSA Team for Verification

The Client identifies the proposed Audit Team Leader, Team Member(s) and any Observers and instructs them to complete the Auditor Verification form. The Client collects this information and sends the completed forms to TfL RSA Team for verification.

TfL does not issue ‘blanket’ approval for Auditors external to TfL. Auditor approval is given on an Audit specific basis following demonstration of relevant Auditor

competency. Previous approval for an Audit on the TLRN is not approval for any subsequent or alternative Audits, all of which will need individual approval.

It is fundamental to the auditing process that no member of the RSA Team has had any design involvement with the measures being audited and will maintain this independence throughout.

The Audit Team will only be made up from individuals that have the necessary qualifications, adequate and relevant training, skills and experience. This will be assessed, without exception, through a formal verification process by way of the submission of the Auditor Verification Form to the TfL Road Safety Audit Manager. Road Safety Audit Teams comprised of highway design engineers with little or no experience of road safety work will not be accepted.

The Audit Team will comprise of at least two persons, one of which will lead the Audit (Team Leader), the other (Team Member) will provide technical expertise to assist the Audit Team Leader.

The **mandatory** minimum qualifications and experience for RSA Team Leader and RSA Team Member positions is as follows:

- Membership or Fellowship of the Chartered Institution of Highways and Transportation's (CIHT) Society of Road Safety Auditors (SoRSA).

- Completion of a 10-day formally structured and recognised Collision Investigation or Road Safety Engineering course (or equivalent 9-day condensed or modular course).

- A minimum of 4 years Collision Investigation or Road Safety Engineering experience (Team Leader), or a minimum of 2 years Collision Investigation or Road Safety Engineering experience (Team Member).

- Audit Team Leader - Completion of at least **5** Road Safety Audits in the past 12 months, and completion of at least **25** Road Safety Audits during their career as either a Team Leader or Team Member. Audit Team Leaders must demonstrate audit experience in a diverse range of Traffic Engineering measures.

- Audit Team Member - Completion of at least **5** Road Safety Audits in the past 24 months as either a Team Leader or Team Member.

- A minimum of 2 days certificated Continued Professional Development (CPD) in the fields of Road Safety Audit, Collision Investigation or Road Safety Engineering in the past 12 months.

In addition to the mandatory qualifications and experience, the following **preferred** experience for RSA Team Leader and RSA Team Member positions is as follows:

- An understanding of Transport for London's Cycle Design Standards.

- An understanding of Transport for London's Motorcycle Design handbook.
- An understanding of Transport for London's Pedestrian Design Guidance.
- An Understanding of Transport for London's Streetscape Manual,
- Training in the needs of vulnerable road users.

Road Safety Auditors should have an understanding of how best practice highway design principles may benefit road safety. It is not intended that Road Safety Auditors have extensive detailed design knowledge. However, they should have a reasonable understanding of design Standards and best practice design principles, and how the application of these can minimise collision risk.

The Auditor Verification Form must demonstrate that all formal members of the Audit Team are current Members or Fellows of the Chartered Institution of Highways and Transportation's (CIHT) Society of Road Safety Auditors (SoRSA), which will be checked. Membership of SoRSA (or equivalent) does not guarantee that Auditors will be given approval in all cases as the Auditor must demonstrate that they have experience relevant to the scheme being audited before approval will be given.

Auditors who are Members of an alternative recognised Professional Institute or Institution specific to Road Safety Audit may be accepted under some circumstances. In this circumstance the Auditor will need to apply for specific exemption which will be assessed on a case by case basis. Auditors who fall under this category should contact TfL RSA for details. Specific exemption may be given in writing by TfL Road Safety Audit Manager only if the Auditor as deemed suitable.

The TfL RSA Team reserves the right to check the validity of any information submitted as part of the verification process. This may include checking education and employment history as deemed appropriate. At the discretion of TfL, candidates may be requested to provide evidence of any document detailed upon the verification form such as Certificates, Audit Reports, Collision Studies and evidence of CPD. It is recommended that candidates retain up-to-date records of experience should this information be requested.

Audit reports completed by Auditors who have not passed this verification process in advance of the RSA being carried out will not be accepted under any circumstances.

0170.2.6. Suitability Approved?

TfL RSA Team assesses the suitability of the proposed Audit Team using the criteria identified in 0170.2.5.

If the answer is YES, please refer to step **0170.2.9**.

If the answer is NO, please refer to step **0170.2.7**.

Depending on the scope of the scheme, TfL RSA may decide to assist the Audit Team in the completion of the Audit. This is to ensure consistency across Audits completed by different suppliers, ensure Audits are completed correctly and to

provide additional information regarding the site and auditing in London generally, which may not be known to the Audit Team. If the TfL Audit Team wish to attend the RSA, this will be notified as part of the verification process.

0170.2.7. Respond to Client

TfL's Road Safety Audit Manager responds to the Client indicating why the proposed Auditor(s) have not been accepted and seeks further clarification or suggests appointing a new Audit Team.

0170.2.8. Provides Clarification or Submit Verification Form for New Audit Team

The Client provides the TfL RSA Team with clarification of the original Audit Team or may submit the Auditor Verification Form for a new Audit Team for verification.

0170.2.9. External Audit Team Approved

The TfL Road Safety Audit Manager informs the Client that the external Audit Team have been accepted to undertake the Audit.

0170.2.10. Desktop Assessment

The appointed Audit Team collects the latest collision data and carries out analysis to ascertain any underlying collision patterns. This data is to be used to determine current safety concerns which may not be discernible from the site visit alone and builds a greater appreciation of the future operation of the proposals. A desktop assessment of the drawings and information supplied is carried out prior to visiting the site.

0170.2.11. Specialist Advisor Required?

If there are any unusual or specialist measures to be audited, then the Audit Team Leader may elect to appoint an appropriate specialist to advise the RSA Team.

The Police and Specialist Advisors do not form part of the formal Audit Team and are not required to be members of SoRSA.

If the answer is YES, please refer to step **0170.2.12**.

If the answer is NO, please refer to step **0170.2.13**.

0170.2.12. Enlist Specialist

Audit Team identifies a Specialist Advisor and obtains their comments, advice and suggestions. It may be necessary to revisit the site together.

0170.2.13. Scheme Post-Construction?

The Audit Team identifies if the scheme has already been constructed and therefore requires a Police visit / comments and a night-time site visit.

If the answer is YES, please refer to step **0170.2.14**.

If the answer is NO, please refer to step **0170.2.15**.

0170.2.14. Arrange Site Visit with the Police

At Stage 3, the Team Leader shall invite representatives from the Police to accompany the Audit Team to offer their views for the Audit. Where it proves not possible to arrange a mutually convenient time, the Police will be invited to submit their views in writing.

At Stage 3 and in addition to the daylight site visit, all members of the Audit Team should visit the site of the scheme together during the hours of darkness to identify hazards particular to night-time operation. Seasonal variation will sometimes necessitate undertaking night-time site visits at a late hour. In such cases, the Team Leader may elect to defer the night time site visit, particularly if the personal safety of the Audit Team is considered to be an issue. When deferring the night-time site visit, the Audit report will be issued in draft form until such time as the night-time site visit is undertaken. Night time site visits may not be deferred for more than three months from the daytime site visit.

Audits completed by Audit Teams external to TfL must obtain the Client Organisations and TfL's Road Safety Audit Managers prior approval if it is decided the site does not require a visit during the hours of darkness. In such instances the reasons for not visiting the site at night must be stated within the Audit report. It should be noted that choosing not to visit the site at night should be adopted only in exceptional circumstances.

0170.2.15. Audit Team Visits Site

At each stage of the Audit process, all members of the Audit Team must visit the site of the scheme together during daylight hours. The Audit Team must consider the measures from the perspective of all the road users that may be anticipated to use the scheme. Where appropriate, a combination of driving, walking and cycling through the scheme may be used to assist their evaluation and ensure that they have a comprehensive understanding and appreciation of the scheme. The Audit Team should also consider the effects of different weather conditions and site conditions that may affect the operation of the scheme.

Where the Audit Team identifies an immediate safety concern, they should notify TfL via Customer Services as soon as reasonably practicable. This is particularly important for problems identified during the Stage 3 RSA process.

The Audit Team Leader liaises with the Client, Police and Specialists Advisors as necessary in order to ensure the Audit report can be appropriately completed. It may be necessary to revisit the site.

0170.2.16. Draft Audit Report

The Audit Team compiles the Audit report at pre-construction, post-construction or Stage 4 using TfL's report templates. The problems and recommendations in the

Audit Report should be set out in a logical sequence. The use of headed sections and the details of those headed sections are at the Audit Team's discretion. The Audit Team must avoid the use of superfluous headings for features or road users for which no issues have been identified.

For consistency, **all RSA reports must use TfL's specific report templates without exception**. It is intended that all suppliers provide reports following the same layout and structure to ensure consistency in delivery. It is acceptable to modify the visual appearance of the front cover to include corporate branding and internal quality assurance information as appropriate. However, the report structure must follow TfL's standard layout must remain unchanged.

RSAs must be concise and understandable by those without a background in the field. The use of complicated engineering terminology should be avoided.

Road Safety issues that are beyond the scope of the RSA but that the Audit Team believes should be brought to the attention of the Client Organisation, may be included within Section 4 of the RSA report. These issues could include areas where repair or renewal may be required, operational concerns or existing poor provision. Such issues should be clearly identified as being beyond the scope of the RSA and should not be integrated into the main Problem and Recommendation section (Section 3) of the report.

Section 4 is not intended as an opportunity to provide a record of inspection of the existing site conditions. Only significant issues should be included as a large number of superfluous issues within this Section may remove focus from the genuine issues of concern. Existing issues and problems outside the geographical extents of the scheme should not normally be included within Section 4, unless they impact directly on the operation or delivery of the scheme.

0170.2.17. Check Audit Report

The draft Audit report shall be distributed amongst other members of the Audit Team to check and provide comments. Any necessary changes to the Audit report will be made, but the Audit Team Leader shall take responsibility for the content of the Audit report.

0170.2.18. Approve Audit Report

The amended draft Audit report will be read by another person beyond the Audit Team, preferably with Road Safety Audit experience, to ensure that the Audit report is understandable by those without a background in the field. The Audit Report approver will not instruct the Audit Team to modify the technical content within Road Safety Audit reports.

The ensure the requirements of this procedure are met, TfL RSA reserves the right to request a draft copy of any Audit report to review prior to it being issued as Final. The Client will be informed as part of the verification process if a draft copy of the Audit is required.

0170.2.19. Issue Final Report

The Audit Team Leader issues the Final Audit report to the Client, and the Designer where appropriate.

A copy of all RSA reports must be sent to the TfL RSA Team at the same time it is issued to the Client in final at TfLSafetyAudit@tfl.gov.uk.

0170.2.20. Seek Response from Designer

The Client sends the Audit report to the Designers and seeks their response to the Audit.

0170.2.21. Respond to Audit Issues

The Designer responds to each problem identified in the Road Safety Audit and this is recorded in the Designer's response areas of the Audit report. The response will contain details of how the problems identified in the Audit report will be resolved. Where the Designer disagrees with the problems or recommendations identified in the Audit report, or decides that the solutions recommended are not appropriate, the response justifies the alternative action to be taken. The Audit report is then signed off by the Designer and sent to the Client for comments.

It should be noted that the Designer must demonstrate due consideration of the problems raised within the RSA report when responding to the RSA report.

0170.2.22. Provide Comments and Return to Audit Team

It is the responsibility of the Client to review the RSA report and ensure that each problem identified is given due consideration by the Designer, adding comments in the relevant sections of the RSA report as appropriate.

The RSA report incorporating the Designer's and Client Organisation's comments is signed off by the Client Organisation and a copy is forwarded to the Audit Team Leader for information.

The Audit report is not an opportunity for the Client and the Designer to document their differences. Any disagreements relating to the progression of the proposals should be discussed and agreed separately. The agreed way forward should be documented within the Designer's response section. The Client Organisation is encouraged to use the Client section to provide background information to complement the Designer's decisions that may be beneficial to those reading the Audit report.

The Client Organisation should familiarise themselves with the requirements of CDM when issuing instructions to the Designer that could constitute a design decision.

The Client Organisation commissions the Design Organisation or others if applicable, in respect of changes required to the scheme arising from the Audit response. A scheme should be submitted for Audit again if significant changes are made to it as a result of an Audit.

The response sections of the Audit report must be completed before the next stage in the scheme's development is begun.

0170.2.23. Save Completed Audit Report and Responses

It is the responsibility of the Client Organisation to retain a copy of the signed final Road Safety Audit Report incorporating the Road Safety Audit Response. Filing and retention arrangements for Road Safety Audits must pay due regard to complying with the Freedom of Information Act. It is the responsibility of any Client Organisation to ensure all Road Safety Audits are retained in accordance with their own Policy.

Outputs:

- Road Safety Audit Report with Designer's Responses and Client Comments

7 Relevant Documentation

- Auditor Verification Form
- Collision Risk in Greater London
- External Audit Brief Checklist
- External Post-Construction Audit Report
- External Pre-Construction Audit Report
- External Stage 4 Audit Report
- Glossary
- Internal Audit Brief Checklist
- Internal Post-Construction Audit Report
- Internal Pre-Construction Audit Report
- Internal Stage 4 Audit Report
- Non-Audit Note

NB: External Parties can also email TfLSafetyAudit@tfl.gov.uk to obtain any relevant documentation.

8 Document Control

Issue	Date	Change Summary	Author	Checker	Approver
Previous version 9 now archived and migrated to new SharePoint platform as version 1 on 26/02/16. Contact QMS@tfl.gov.ukto access archived versions.					
1	26/02/2016	Update onto new template. Process updated following revision.	L Pan (Highways Specialist Engineer)	B Schoenmakers (AMD QMS Support)	A Coventry (Road Safety Audit Manager)

Transport for London

Invitation to Quote

Electric Vehicle Infrastructure Delivery (EVID)
Tranche 2, Batch 1

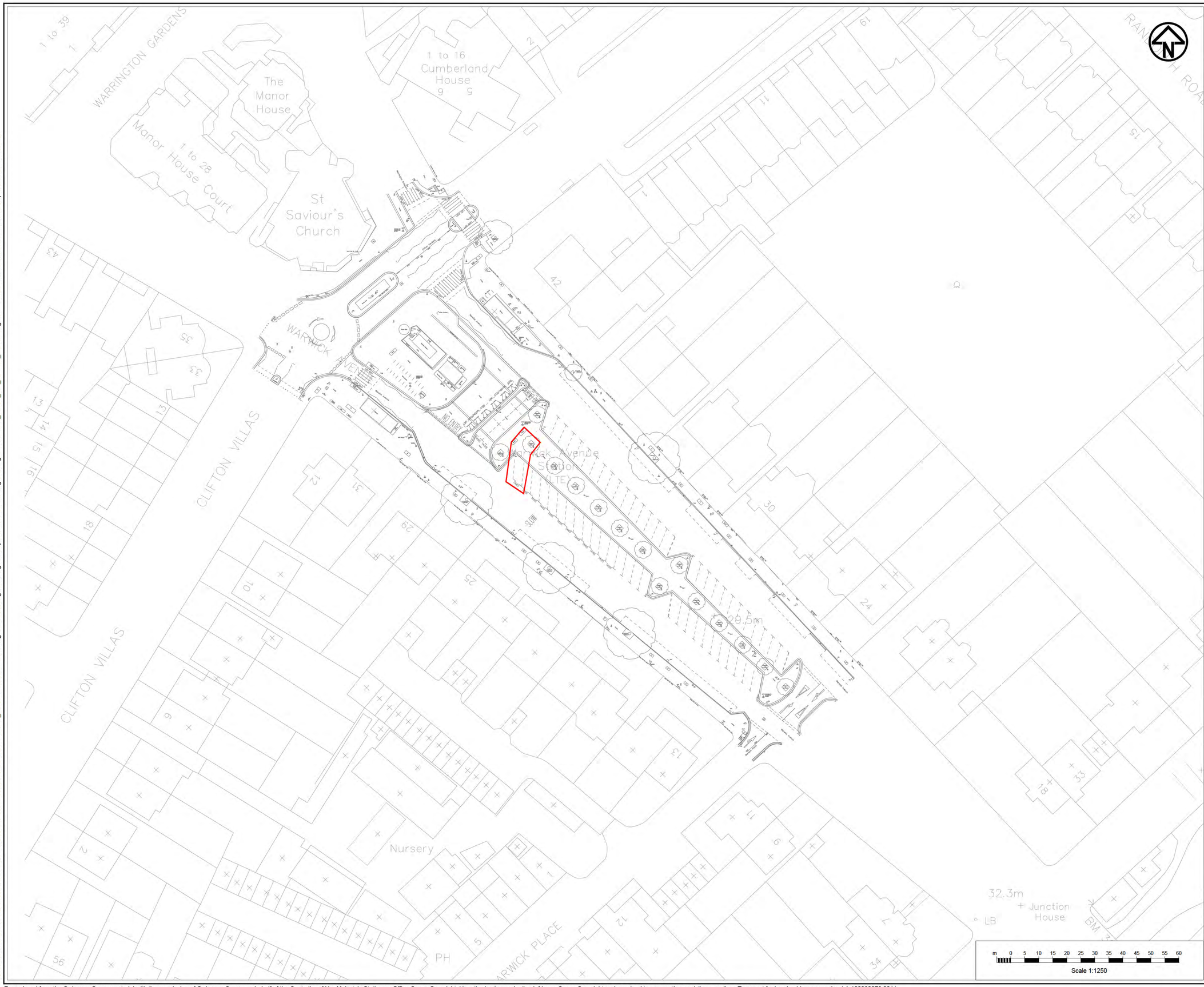
Volume 2

Appendix I_1

Example site location plan – Warwick Avenue

COMMERCIAL IN CONFIDENCE

TfL Restricted



Notes

1. All dimensions are in metres unless otherwise stated. Dimensions shown are for illustrative purposes. Contractor is to refer to relevant drawings for setting out details.
2. Do not scale from this drawing.
3. Layouts are a combination of both topographical survey and Ordnance Survey. Where topographical survey information is not provided on drawings, all dimensions shown have been measured on site. Clarification and discrepancies to be brought to the attention of the Site Engineer.

Key:

Application Site

REV	REV. DATE	PURPOSE OF REVISION	DRAWN	CHKD	APPRVD
06	12/09/2018	VIEWPORT REMOVED	RCM	AG	NM
05	04/06/2018	MINNOR AMENDMENT	UF	RCM	NM
04	21/05/2018	RELOCATE FP & PLANT NEW TREE	UF	RCM	NM
03	09/05/2018	RELOCATE FP TO NEW LOCATION	UF	RCM	NM
02	08/05/2018	NEW 2 no. PARKING BAYS	UF	RCM	NM
01	01/05/2018	PROPOSED NEW EV BAY BUILT-OUT	UF	RCM	NM
00	05/04/2018	FOR PLANNING APPLICATION	RCM	UF	NM

RINGWAY JACOBS

integrated with LONDON HIGHWAYS ALLIANCE

FOR PLANNING ONLY

Project

RAPID CHARGING INFRASTRUCTURE
WESTMINSTER - SITE ID: 174
OPPOSITE 27 WARWICK AVENUE

Drawing Title

SITE LOCATION PLAN

Drawing Status

FOR PLANNING APPLICATION

Scale	1:1250 @ A3	DO NOT SCALE
Ringway Jacobs No.	NE2017_0190P	
Client No.	NE2017_0190P	

Drawing Number: NE2017_0190P_174_101 — Rev: 06

This drawing is not to be used in whole or part other than for the intended purpose and project as defined on this drawing. Refer to the contract for full terms and conditions.

File location: \\UKBRISTCSFP0000\Tfl\L01 LoHAC\03 LoHAC Schemes\05. Year 5 - 2017\NE2017_0190P - RCI Batch 9 Investigations\02 Design Drawings and Specification\03 Working Drawings\174\NE2017_0190P_174_101-103_REV06.dwg-101 User: Roberto Merchan Time: 12 September 2018 14:35:30

Reproduced from the Ordnance Survey material with the permission of Ordnance Survey on behalf of the Controller of Her Majesty's Stationery Office Crown Copyright. Unauthorised reproduction infringes Crown Copyright and may lead to prosecution or civil proceedings.Transport for London Licence number LA 100032379 2011

Transport for London

Invitation to Quote

Electric Vehicle Infrastructure Delivery (EVID)
Tranche 2, Batch 1

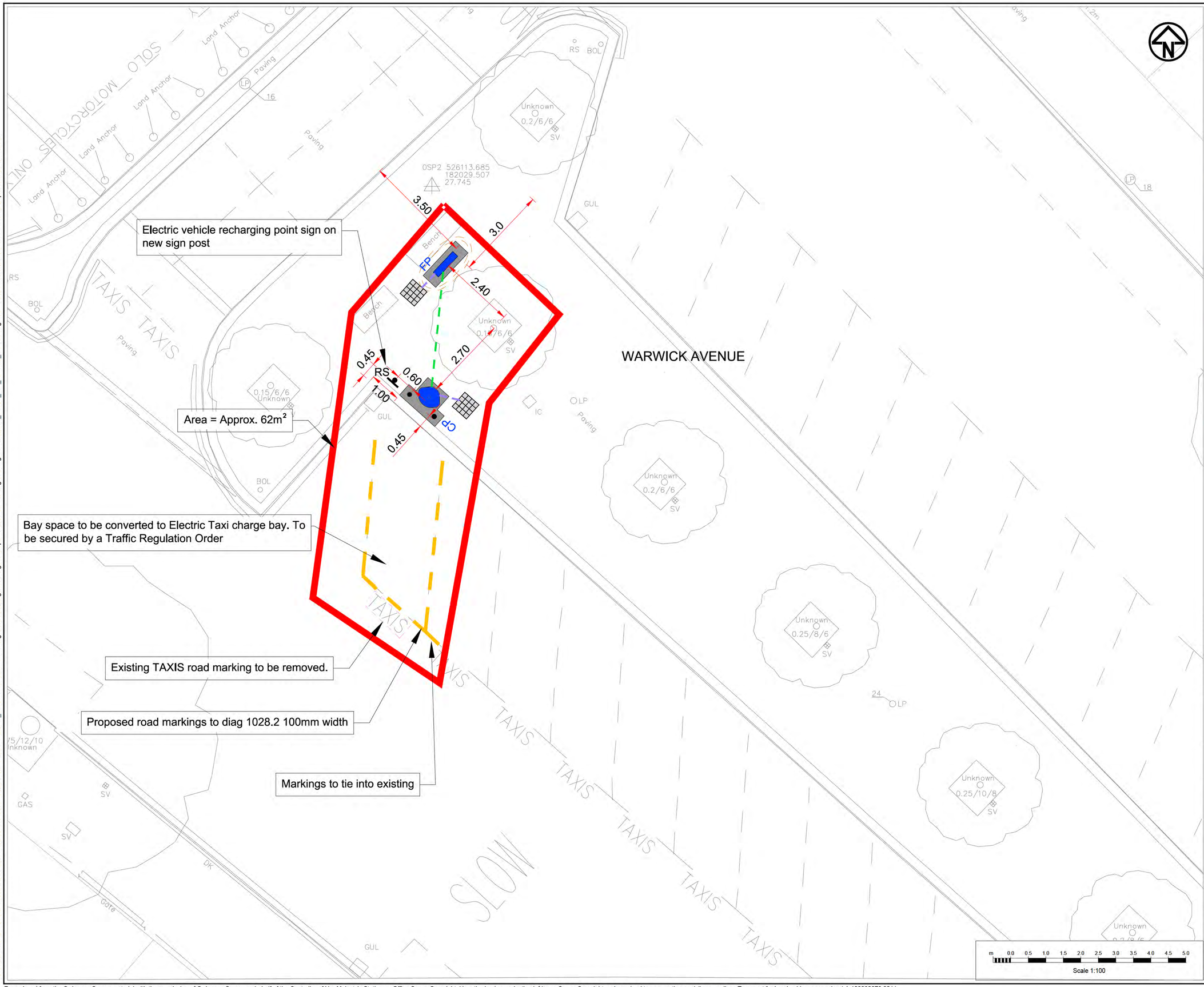
Volume 2

Appendix I_2

Example proposed layout – Warwick Avenue

COMMERCIAL IN CONFIDENCE

TfL Restricted



Notes

1. All dimensions are in metres unless otherwise stated. Dimensions shown are for illustrative purposes. Contractor is to refer to relevant drawings for setting out details.
2. Do not scale from this drawing.
3. Layouts are a combination of both topographical survey and Ordnance Survey. Where topographical survey information is not provided on drawings, all dimensions shown have been measured on site. Clarification and discrepancies to be brought to the attention of the Site Engineer.

Key:

- CP — Proposed Rapid Charging Point.
- FP — Proposed Feeder Pillar.
- Proposed earth mat, 600mm x 600mm with marconite surround. Location to be confirmed on site.
- RS — Proposed road sign.
- Proposed Electric Taxi bay 100mm wide intermittent line in Yellow.
- Proposed parking bay 100mm wide intermittent line in white.
- Proposed ducting 100mm dia in black at 450mm depth. Location to be determined on site.
- Proposed flexi-duct Ø50mm black at 450mm depth with 16mm² copper cable for earthing. Location to be confirmed on site.
- Existing Road Markings to be removed by hydroblasting.
- Application Site.
- Bollard

REV	REV. DATE	PURPOSE OF REVISION	DRAWN	CHKD	APPRVD
06	12/09/2018	VIEWPORT REMOVED	RCM	AG	NM
05	04/06/2018	MINNOR AMENDMENT	UF	RCM	NM
04	21/05/2018	RELOCATE FP & PLANT NEW TREE	UF	RCM	NM
03	09/05/2018	RELOCATE FP TO NEW LOCATION	UF	RCM	NM
02	08/05/2018	NEW 2 no. PARKING BAYS	UF	RCM	NM
01	01/05/2018	PROPOSED NEW EV BAY BUILT-OUT	UF	RCM	NM
00	05/04/2018	FOR PLANNING APPLICATION	RCM	UF	NM

RINGWAY JACOBS
Integrated delivery
LONDON HIGHWAYS ALLIANCE

FOR PLANNING ONLY

Project
RAPID CHARGING INFRASTRUCTURE
WESTMINSTER - SITE ID: 174
OPPOSITE 27 WARWICK AVENUE

Drawing Title
PROPOSED LAYOUT

Drawing Status
FOR PLANNING APPLICATION

Scale	1:100 @ A3	DO NOT SCALE
Ringway Jacobs No.	NE2017_0190P	
Client No.	NE2017_0190P	

Drawing Number: NE2017_0190P_174_103 — Rev: 06

This drawing is not to be used in whole or part other than for the intended purpose and project as defined on this drawing. Refer to the contract for full terms and conditions.

File location: \\UKBRISTCSFP0000\TfL\01 LoHAC\03 LoHAC Schemes\05. Year 5 - 2017\NE2017_0190P - RCI Batch 9 Investigations\02 Design Drawings and Specification\03 Working Drawings\174\NE2017_0190P_174_101-103_REV06.dwg-103 User: Roberto Merchan Time: 12 September 2018 14:36:21

Reproduced from the Ordnance Survey material with the permission of Ordnance Survey on behalf of the Controller of Her Majesty's Stationery Office Crown Copyright. Unauthorised reproduction infringes Crown Copyright and may lead to prosecution or civil proceedings.Transport for London Licence number LA 100032379 2011

Transport for London

Invitation to Quote

Electric Vehicle Infrastructure Delivery (EVID)
Tranche 2, Batch 1

Volume 2

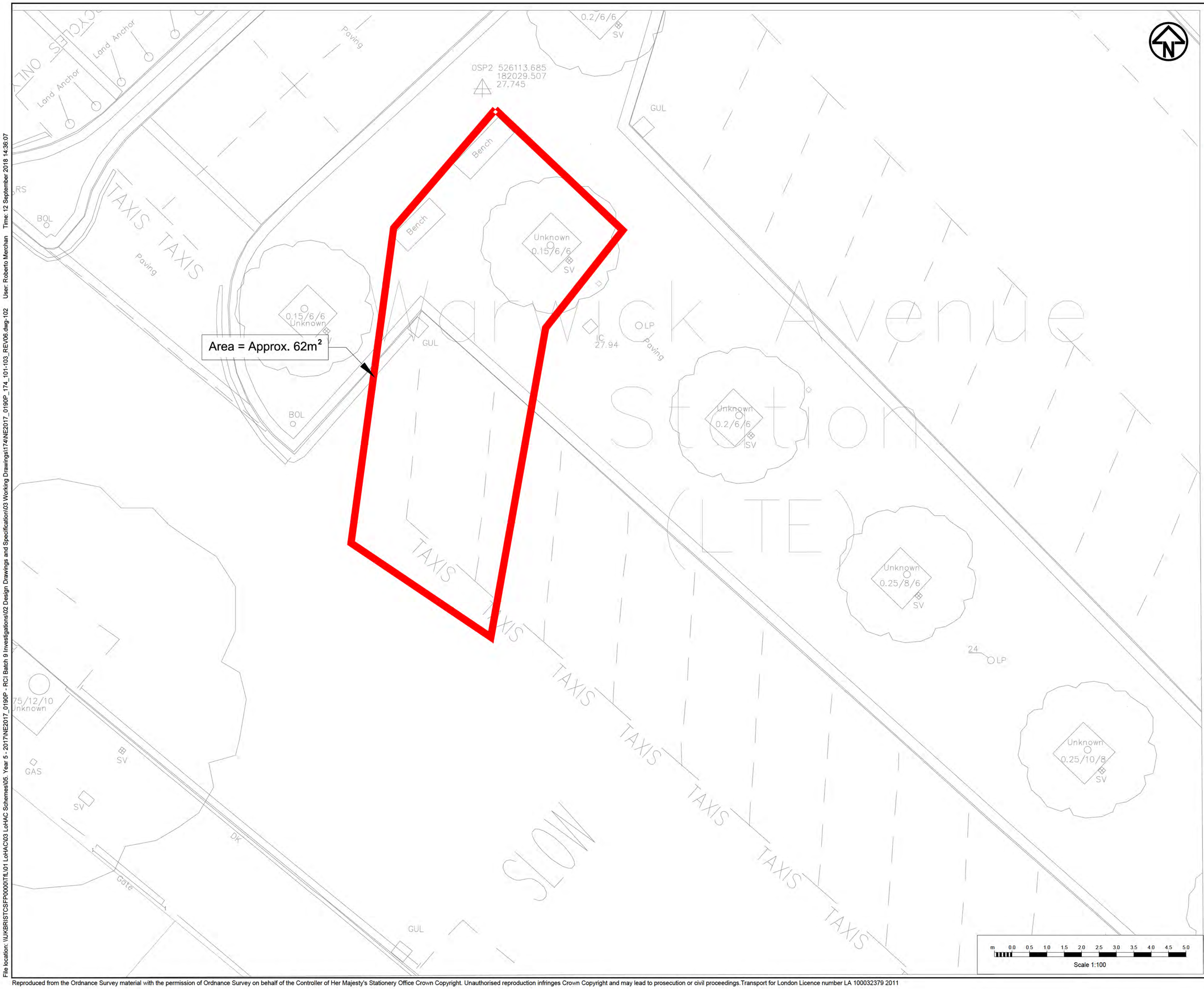
Appendix I_3

Example existing layout – Warwick Avenue

COMMERCIAL IN CONFIDENCE

TfL Restricted

File location: \\UKBRISTCSFP0000\Tfl\01 LoHAC\03 LoHAC Schemes\05. Year 5 - 2017\NE2017_0190P - RCI Batch 9 Investigations\02 Design Drawings and Specification\03 Working Drawings\174\NE2017_0190P_174_101-103_REV06.dwg-102 User: Roberto Merchan Time: 12 September 2018 14:36:07



Notes

1. All dimensions are in metres unless otherwise stated. Dimensions shown are for illustrative purposes. Contractor is to refer to relevant drawings for setting out details.
2. Do not scale from this drawing.
3. Layouts are a combination of both topographical survey and Ordnance Survey. Where topographical survey information is not provided on drawings, all dimensions shown have been measured on site. Clarification and discrepancies to be brought to the attention of the Site Engineer.

Key:

- Application Site
- Existing Road Marking
- LP — Existing Lamp Column
- RS — Existing Road Sign
- GUL — Existing Gully
- Existing Bike Stands
- BOX — Existing Box
- XX — Statutory undertakers cover (text may show IC, TP, WM, FH, SV, CATV or GAS)

REV	REV. DATE	PURPOSE OF REVISION	DRAWN	CHKD	APPRVD
06	12/09/2018	VIEWPORT REMOVED	RCM	AG	NM
05	04/06/2018	MINNOR AMENDMENT	UF	RCM	NM
04	21/05/2018	RELOCATE FP & PLANT NEW TREE	UF	RCM	NM
03	09/05/2018	RELOCATE FP TO NEW LOCATION	UF	RCM	NM
02	08/05/2018	NEW 2 no. PARKING BAYS	UF	RCM	NM
01	01/05/2018	PROPOSED NEW EV BAY BUILT-OUT	UF	RCM	NM
00	05/04/2018	FOR PLANNING APPLICATION	RCM	UF	NM

RINGWAY JACOBS
integrated with LONDON HIGHWAYS ALLIANCE

FOR PLANNING ONLY

Project
RAPID CHARGING INFRASTRUCTURE
WESTMINSTER - SITE ID: 174
OPPOSITE 27 WARWICK AVENUE

Drawing Title
EXISTING LAYOUT

Drawing Status
FOR PLANNING APPLICATION

Scale	1:100 @ A3	DO NOT SCALE
Ringway Jacobs No.	NE2017_0190P	
Client No.	NE2017_0190P	
Drawing Number	NE2017_0190P_174_102	Rev 06

This drawing is not to be used in whole or part other than for the intended purpose and project as defined on this drawing. Refer to the contract for full terms and conditions.

Reproduced from the Ordnance Survey material with the permission of Ordnance Survey on behalf of the Controller of Her Majesty's Stationery Office Crown Copyright. Unauthorised reproduction infringes Crown Copyright and may lead to prosecution or civil proceedings.Transport for London Licence number LA 100032379 2011

Transport for London

Invitation to Quote

Electric Vehicle Infrastructure Delivery (EVID)
Tranche 2, Batch 1

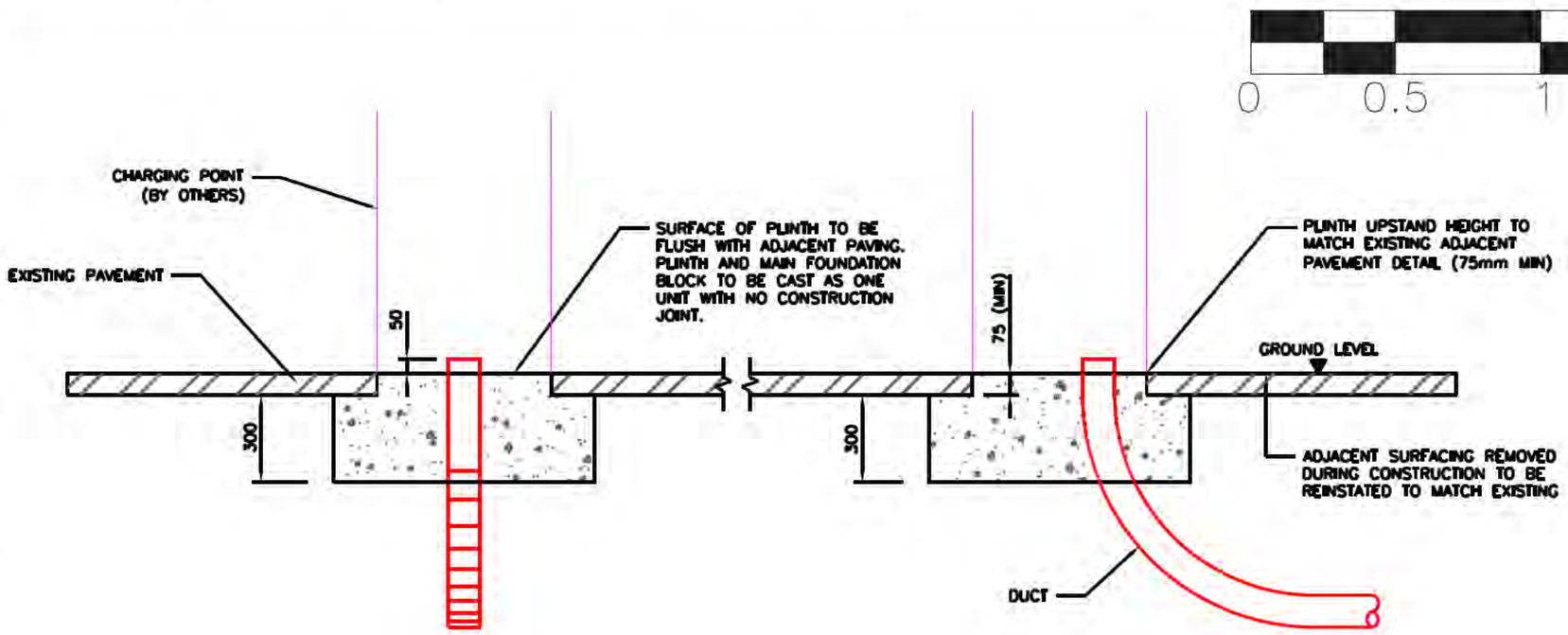
Volume 2

Appendix I_4

Example foundation design drawing

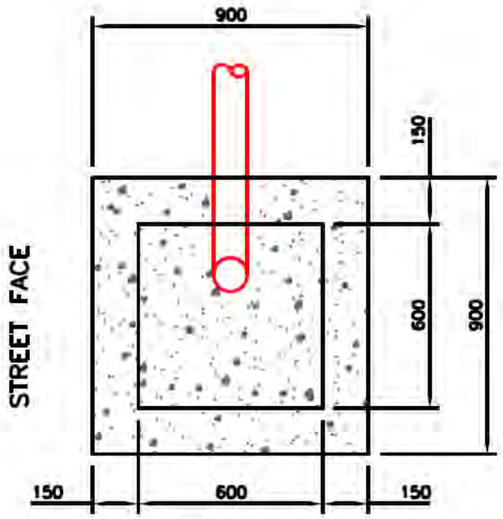
COMMERCIAL IN CONFIDENCE

TfL Restricted

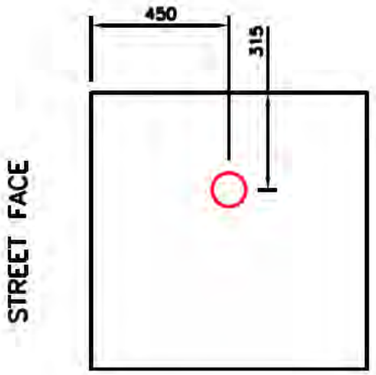


ELEVATION
SCALE 1:20

END VIEW
SCALE 1:20



PLAN
SCALE 1:20



DUCT LOCATION PLAN
SCALE 1:20

NOTES:

FOUNDATION CONCRETE TO BE CEM I CONCRETE OF COMPRESSIVE STRENGTH CLASS C30/37 WITH A MAX. WATER:CEMENT RATIO OF 0.5.

TOP SURFACE OF THE CONCRETE TO HAVE A CLASS U3 FINISH. BURIED SIDES OF THE CONCRETE TO HAVE A CLASS F1 FINISH.

THE DUCT SHALL BE POSITIONED IN THE FOUNDATION AS SHOWN. DUCTING DIRECTION SHALL BE AS GIVEN ON THE LAYOUT DRAWINGS

SUBGRADE AT FORMATION LEVEL TO BE CLEAN AND FREE FROM LOOSE MATERIAL OR DEBRIS. SUBGRADE TO HAVE A MINIMUM BEARING CAPACITY OF 30kPo. UNSUITABLE MATERIAL SHALL BE EXCAVATED AND REPLACED WITH LEAN MIX CONCRETE OR CLAUSE 803 MATERIAL, AS DIRECTED BY THE ENGINEER.

DESIGN ASSUMES MINIMAL HORIZONTAL LOADS. IF HORIZONTAL LOADS OTHER THAN WIND LOADING OR LATERAL LOADING OF 0.9kN AT 1.2m ABOVE GROUND LEVEL ARE EXPECTED PLEASE CONSULT THE ENGINEER.

SAMPLING AND TESTING FOR COMPRESSIVE STRENGTH TO BE CARRIED OUT IN ACCORDANCE WITH ANNEX B OF BS EN 206-1 AND ANNEX B OF BS 8500-1. 1 SAMPLE OF 3 CUBES IS TO BE TAKEN FOR EACH FOUNDATION. 1 CUBE IS TO BE TESTED AT 7 DAYS AND 2 CUBES AT 28 DAYS.

SAMPLING AND TESTING FOR CONSISTENCY (SLUMP TEST) IS TO BE CARRIED OUT IN ACCORDANCE WITH ANNEX B OF BS 8500-1. 1 SLUMP TEST IS TO BE CARRIED OUT FOR EACH CONCRETE DELIVERY.

ANCHOR BOLTS FOR CHARGE POINT CABINET ARE TO BE POST FIXED BY OTHERS.

Rev.	Date	Revision Description	Drn.	Prod.	Ver.	App.
000	08/2017	Initial Version	BC	BC	JM	ES

Purpose of issue - Preliminary unless indicated
Tender ☐ Client Approval ☐ Construction ☐ As-built ☐ Revised ☐

Energy for generations
ESB Innovation, Two Gateway, East Wall Road, Dublin D03 A995 Ireland. **Tel:** +353 (0)1 676 5831 **Fax:** +353 (0)1 703 8088
Email: ecars@esb.ie **Web:** www.esb.ie

Client

Project: Transport for London RCP Framework

Contract: -

Production Unit: ESB eCars

Drawing Title: Rapid Charge Point Installation
Efacec QC45 Foundation

Detailed Civil Design

Standard Drawing

COPYRIGHT © ESBI ENGINEERING & FACILITY MANAGEMENT LIMITED.
All rights reserved. No part of this work may be modified or reproduced or copied in any form or by any means - graphic, electronic or mechanical, including photocopying, recording, taping or information-and-retrieval system, or used for any purpose other than its designated purpose, without the written permission of ESBI Engineering & Facility Management Ltd.

DRAWN	PRODUCED	VERIFIED	APPROVED	APPROVAL DATE
B.Carroll	B.Carroll	J. Mooney	E. Silke	15/08/2017

CLIENT REF	No. of Shts	SIZE	SCALE
Client Reference No.	1	A3	1:20

Drawing Number: ESB-001-011-000 SHEET REV

Transport for London

Invitation to Quote

Electric Vehicle Infrastructure Delivery (EVID)
Tranche 2, Batch 1

Volume 2

Appendix I_5

Example charge point design drawing

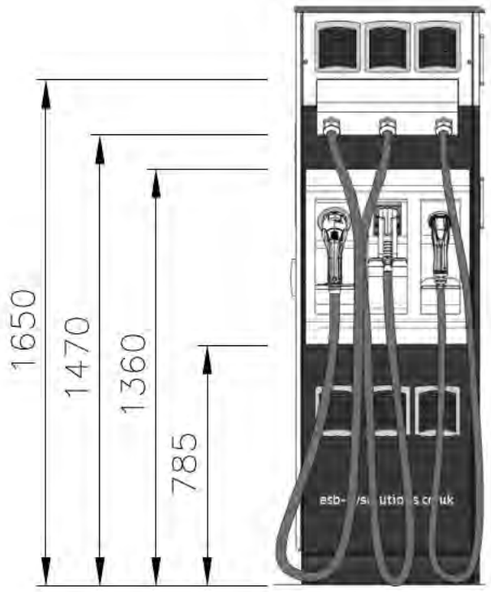
COMMERCIAL IN CONFIDENCE

TfL Restricted

SIDE A
(UI)



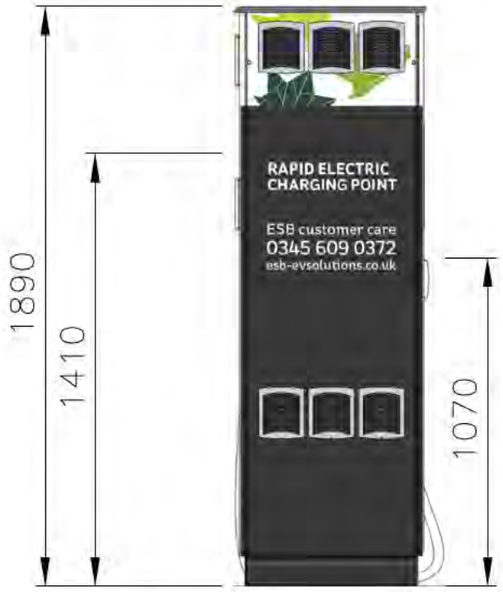
SIDE B

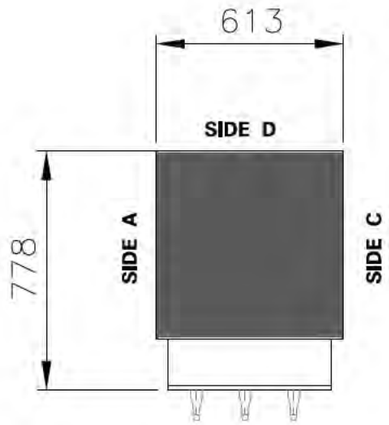


SIDE C



SIDE D





RAPID ELECTRIC CHARGING POINT
CLEANERAIR FOR LONDON
MAYOR OF LONDON
City of Westminster
TRANSPORT FOR LONDON
EVERY JOURNEY MATTERS

MATERIALS

Galvanized mild steel coated in a protective paint as standard.
These comply with the paint protection rating of ISO12944-2 class C4M.
Branded PVC Film Wrap Orajet-3651, Anti-Graffiti Coating.

CHARGE POINT
POLYESTER POWDER COATING
RAL 9005 (BLACK)

0 0.5 1 2 5

Rev.	Date	Revision Description	Drn.	Prod.	Ver.	App.
003	07/2018	Branding revised	RW	RW	BC	ES
002	01/2018	Branding revised	RW	RW	BC	ES
001	10/2017	Branding revised	RB	RB	BC	ES
000	09/2017	Initial Version	BC	BC	MOD	ES

Purpose of issue - Preliminary unless indicated
Tender ☒ Client Approval ☐ Construction ☐ As-built ☐ Revised ☐

Energy for generations
ESB Innovation, Two Gateway, East Wall Road, Dublin D03 A995 Ireland. **Tel:** +353 (0)1 676 5831 **Fax:** +353 (0)1 703 8088
Email: ecars@esb.ie **Web:** www.esb.ie

Client

Project: Transport for London

Contract: SS/CON/3158-007

Production Unit: ESB eCars

Drawing Title: Rapid Charge Point Installation
Transport for London
Efacec QC45 Scale Design Drawings
3 Connector Multi-Standard
Elevation View

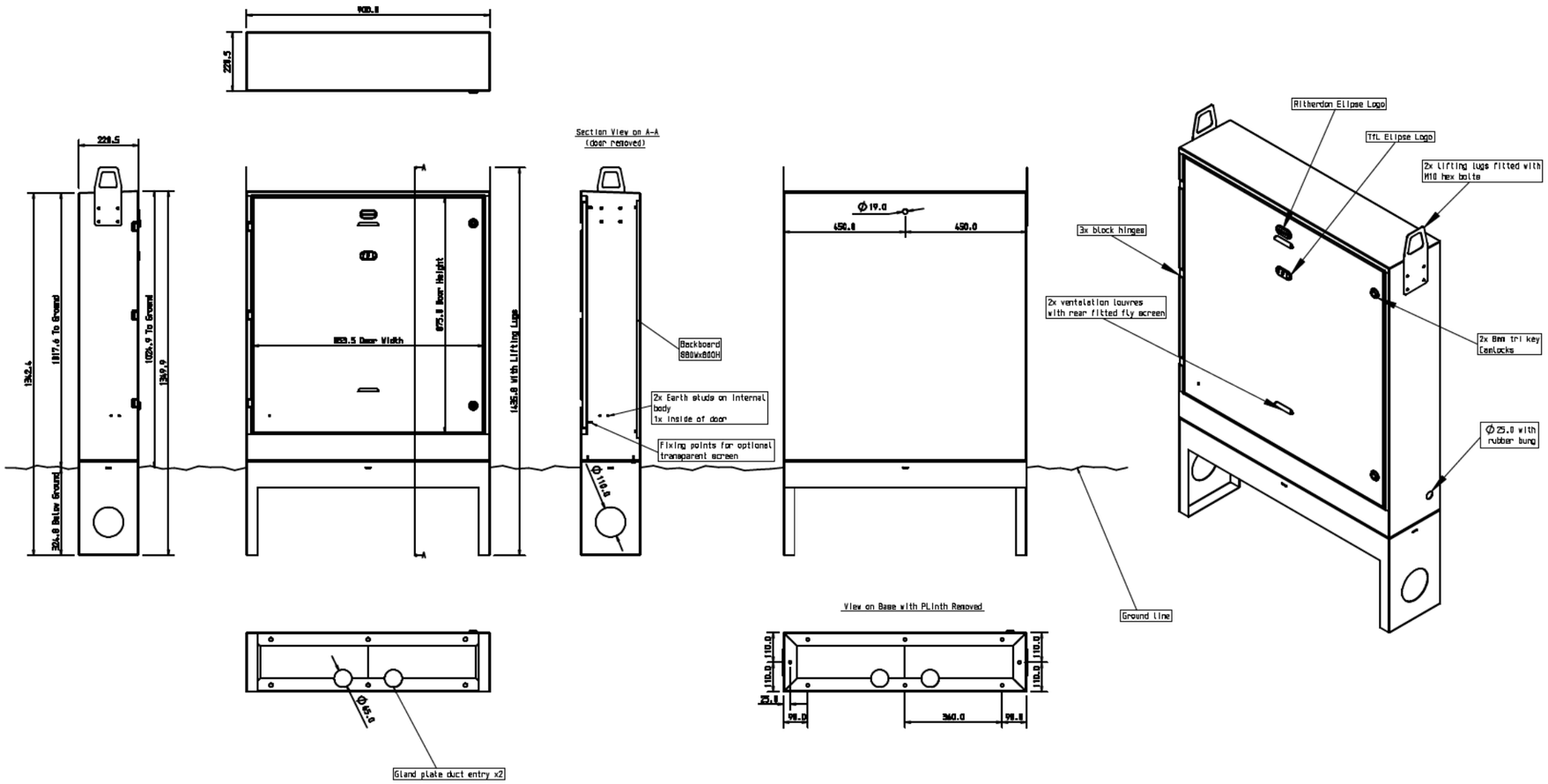
COPYRIGHT © ESBI ENGINEERING & FACILITY MANAGEMENT LIMITED.
All rights reserved. No part of this work may be modified or reproduced or copied in any form or by any means - graphic, electronic or mechanical, including photocopying, recording, taping or information-and-retrieval system, or used for any purpose other than its designated purpose, without the written permission of ESBI Engineering & Facility Management Ltd.

DRAWN	PRODUCED	VERIFIED	APPROVED	APPROVAL DATE
R.Wilson	R.Wilson	B.Carroll	E.Silke	13/07/2018

CLIENT REF | No. of Shts: 1 | SIZE: A3 | SCALE: 1:20

Drawing Number: ESB-001-010-003 | SHEET | REV

A3



DRAWN	Josh Eastham	DATE	23 . 08 . 2017
CHECKED	Mark Blease	DATE	23 . 08 . 2017
APPROVED	Mark Blease	DATE	23 . 08 . 2017

ISSUE	DATE	MOD. NO.	DRN

RITHERDON

COPYRIGHT IS STRICTLY RESERVED

TOLERANCES
WHOLE NUMBERS +/- 0.5
1 DECIMAL PLACE +/- 0.2
HOLES +/- 0.15
UNLESS OTHERWISE STATED

ALL OUTSIDE SIZES

MATERIAL: Stainless Steel

FINISH: RAL 9005 Black Anti-Graffiti Leatherette

TITLE: TfL RH900 Type C General Arrangment

SCALE	DRAWING NO.	[SHEET]	ISSUE
1:20 at A3	S 9840	2	-

Transport for London

Invitation to Quote

Electric Vehicle Infrastructure Delivery (EVID)
Tranche 2, Batch 1

Volume 2

Appendix J

Notice Template

COMMERCIAL IN CONFIDENCE

TfL Restricted

Transport for London

INSERT DATE HERE

NOTICE UNDER SECTION 17 OF THE LONDON LOCAL AUTHORITIES AND TRANSPORT FOR LONDON ACT 2013

Transport for London in partnership with London Borough of (XXXXXX) under section 16(2) of the London Local Authorities and Transport for London Act 2013 are seeking to grant (INSERT CONCESSIONAIRE HERE) permission to provide and operate charging apparatus for electrically powered motor vehicles on the on the footway outside (INSERT ADDRESS HERE) Specifically, the charging apparatus scheme is to involve the installation of (XX) Rapid Charge Point(s) and an associated feeder pillar(s).

INSERT PLAN EXTRACT HERE

SAMPLE

In accordance with section 17(5) of the London Local Authorities and Transport for London Act 2013, representations in respect of the proposed scheme may be made via the following:

Email: EVIDProject@tfl.gov.uk
Postal Address: EVID Project
197 Blackfriars Rd,
Palestra, Southwark,
London SE1 8NJ

Representations are to be made through the period commencing DAY MONTH YEAR and ending DAY MONTH YEAR inclusive. All representations will be considered by Transport for London.

Transport for London

Invitation to Quote

Electric Vehicle Infrastructure Delivery (EVID)
Tranche 2, Batch 1

Volume 2

Appendix K1

Operational Technology Cyber Security- Projects and Upgrades

COMMERCIAL IN CONFIDENCE

TfL Restricted

Standard

S1771 A1 Operational Technology Cyber Security - Projects and Upgrades

Contents

1 Purpose 3

2 Scope 3

2.1 Operation Technology (OT) definition 3
2.2 Examples 4

3 Requirements 5

3.1 Protecting against cyber attack 6
3.2 Detecting cyber security events 6
3.3 Minimising the impact of cyber security incidents 7

4 OT Project Lifecycle 7

4.1 OT Project Lifecycle 7
4.2 Good Practice Principles 8
4.3 OT Project Lifecycle Requirements 8
4.4 The Purdue model and Secure OT Design 15

5 Protecting against cyber attack 15

5.1 Identity and access control 15
5.2 Data Security 21
5.3 Personnel Security 24
5.4 Physical Security 26
5.5 Network Security 28
5.6 System Security 32
5.7 Secure Management: 41

6 Detecting cyber security events 41

6.1 Security Monitoring 42

7 Minimising the impact of cyber security incidents 46

7.1 Incident response and recovery planning 46
7.2 Backups: 48
7.3 Incident lessons learned 48

8 Supporting Information 49

8.1 Background 49
8.2 Customer Considerations 49

MAYOR OF LONDON
Transport for London
TfL RESTRICTED

9 Guidance 49
10 Person accountable for this document 49
11 Definitions 49
12 Abbreviations 50
13 References 50
14 Document history 51

MAYOR OF LONDON
Transport for London
TfL RESTRICTED

1 Purpose

This standard describes the cyber security requirements relating to the design, build, testing, implementation and handover to operations for all new projects and system upgrades comprising or containing Operational Technology (OT) in Transport for London (TfL).

2 Scope

This standard applies to TfL staff and partners with responsibility for designing and implementing OT throughout the lifecycle of any project relating to OT.

2.1 Operation Technology (OT) definition

Operational Technology is a collection of personnel, processes, hardware, and software that can affect or influence the safe, secure, and reliable operation of a physical process or asset.

These include, but are not limited to:

- Signalling for rail, road and marine transport, train management, Supervisory Control and Data Acquisition (SCADA), building management and access control, Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), intelligent electronic devices, networked electronic sensing and control, and monitoring and diagnostic systems.

In this context, process control systems include basic process control system and Safety-Instrumented System (SIS) functions, whether they are physically separate or integrated.

- Associated information systems such as advanced control, dedicated equipment monitors, graphical interfaces, process historians, and plant information management systems.
- Associated internal, human, network, or machine interfaces used to provide monitoring, control, and safety operations functionality.

As an owner and operator of physical transport assets, TfL has an extensive estate of OT systems and devices across a wide range of its underground and surface operations.

There are OT systems which are clearly OT such as traction power, tunnel ventilation, fire detection, and systems which are clearly Information Technology (IT) such as Human Resources (HR) and email. However, there are systems where the distinction is not as clear, such as CCTV and ticket barriers.

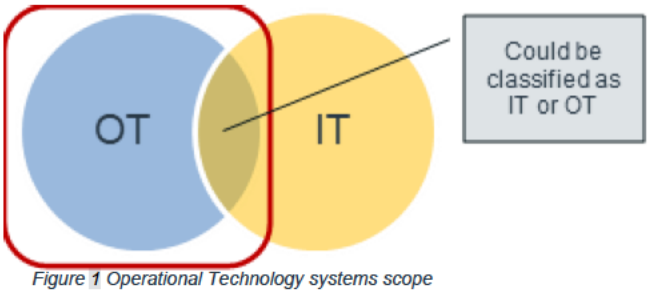


Figure 1 Operational Technology systems scope

MAYOR OF LONDON
Transport for London
TfL RESTRICTED

2.2 Examples

In this section we provide some examples of systems which may or may not be considered or recognised as OT.

2.2.1 Example OT systems

Examples of OT systems installed in London Underground and Surface Transport that are clearly OT include, but is not limited to:

- Power management systems (traction and general power)
- Energy monitoring
- Signalling systems
- Road traffic signals
- Rolling stock
- Communication networks used by OT (e.g. Surface WAN/Connect/Station LAN)
- Control and information systems
- Track systems
- Station systems (e.g. escalator and elevator control)
- Fire detection and suppression systems
- Civil Systems / Tunnel Systems
- Building management systems and building automation systems
- Heating, ventilation and air conditioning (HVAC) systems
- Security and access control systems (e.g. swipe card or key fob)

2.2.2 Example of systems which can be OT or IT

Some systems may be defined as OT or IT, which is usually dependent on the context. To determine if the system is OT or IT, refer to the definition in section 2.1 above and apply the test of whether the systems "can affect or influence the safe, secure, and reliable operation of a physical process or asset." If the answer to this is "Yes", then the system is OT, otherwise it is IT. If the answer is not clear, then refer to the supporting bullet points in the definition to for tests, such as whether the system provides "sensing" or "control", for example.

Some common edge cases which may be classified as OT or IT are given below:

CCTV and One Person Operation (OPO) CCTV – If the CCTV system (cameras and recorders) are networked then they would come under the definition as "networked electronic sensing" and "monitoring" in the definition above. CCTV which is monitoring an area (e.g. an underground station platform) controlled by other OT (e.g. BMS or signalling) should be classified as OT. CCTV which is not used directly to deliver or support delivering a service (e.g. Head Office CCTV for security monitoring) should be classified as IT.

Lighting controls – Simple manual lighting controls are unlikely to be OT. Automated, remotely controlled or monitored lighting control systems for stations, road and rail tunnels, ferry terminals, are likely to be OT as they can affect the reliable operation of the lighting and of services.

HVAC – Reasonably modern HVAC systems in stations, tunnels and buildings (e.g. Victoria coach station) will have a control system which may be linked into a BMS. They may also have remote access from a facilities management and/or maintenance company.

Ticket barriers – A particular physical access control system which not only has card readers and controllers (OT) but will also link to ticketing systems which will be in the IT network.

Timetabling – Scheduling bus and train services with the timetabling system (IT) may need to interface to other OT systems, such as train management systems. The timetabling system would not be classified as OT because it does "affect or influence the safe, secure, and reliable operation" of services.

2.2.3 Alignment to Purdue Model

A complementary approach to determining if a system should be defined as OT or IT is to refer to the Purdue Model, G1771 Section 4.4.1 refers, where OT systems and services sit in Levels 0 to 3 in the Model and IT systems and services sit in Levels 4 and 5 of the Model.

3 Requirements

This standard details the mandatory requirements for OT cyber security through Projects and Upgrades and is aligned to the Network and Information Systems (NIS) Regulations (2018) and the International Electrotechnical Commission IEC 62443 series of standards for OT cyber security, in particular IEC 62443-3-3 system security requirements and security levels. It forms part of a wider framework of standards and guidance (R1770) for OT cyber security in TfL. The standard should be read in tandem with the associated guidance (G1771).

Each system must be subject to a risk assessment to determine its cyber risk and to identify any additional controls required above that of the established minimum-security baseline or concessions which might be necessary where the minimum baseline cannot be met.

Notwithstanding this, the minimum cyber security baseline established within this standard is the set of minimum cyber security requirements for ALL new or upgraded OT which support TfL services.

The baseline is intended to prevent the unauthorised disclosure of information to an entity actively searching for it using simple means with low resources, generic skills, and low motivation. These requirements are applicable to all OT assets including, but not limited to, Intelligent Electronic Devices, RTUs, Microcontrollers, PLCs, Sensors, Actuators, Servers, Workstations, and Network Devices.

Concessions or non-compliance to the requirements established within this standard must have appropriate mitigating controls implemented and follow the formal engineering concession process. Any risks arising from the concession must have

MAYOR OF LONDON
Transport for London
TfL RESTRICTED

been registered in the project risk register, which is then transferred to the system owner and maintained as the system risk register.

The standard is intended to direct staff and partners working for TfL to understand and adopt the necessary steps to protect against cyber threats, detect a cyber incident and respond to a cyber incident when designing and implementing OT which supports the delivery of TfL services safely and reliably.

Not all elements of the standard are solely the responsibility of the project team responsible for the respective OT system; in some areas, TfL will have to have organisational processes or shared services, such as monitoring, in place to support these requirements and the OT systems will have to have the capabilities to apply the requirements.

For example, if an individual moves role, there needs to be recognition at an organisational level that their access privileges must be reviewed, but the system must have appropriate mechanisms to ensure access controls can be enforced and updated.

It is important to note that this standard closely mirrors Operational Technology Cyber Security – Operations and Maintenance (S1772) and the two documents have been written in parallel.

The key difference is that for Operations and Maintenance the emphasis is on **operating** and **supporting** the OT securely and according to established process to limit the likelihood and impact of a cyber incident, so the broader guidance remains to give context and build understanding of why the security controls are important. For Projects and Upgrades, the emphasis is more focused on **designing** and **implementing** the OT in a secure way, such that the cyber risk is mitigated as far as practicable and that the controls are appropriate to the risk.

Cyber security considerations or controls are grouped according to the following security principles and the components of each phase are explained in the following sections.

3.1 Protecting against cyber attack

The requirement is that TfL and partners will have proportionate security measures in place to protect TfL services and systems from cyber-attack.

The underlying principle is that TfL defines, implements, communicates, and enforces appropriate policies and processes that direct its overall approach to securing systems and data that support delivery of TfL services.

3.2 Detecting cyber security events

The requirement is that TfL and partners will have the capabilities to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, TfL services.

The underlying principle is that TfL monitors the security status of the networks and systems supporting the delivery of TfL services to detect potential security problems and to track the ongoing effectiveness of protective security measures.

MAYOR OF LONDON
Transport for London
TfL RESTRICTED

3.3 Minimising the impact of cyber security incidents

The requirement is that TfL and partners will have the capabilities to minimise the impact of a cyber security incident on TfL services, including the restoration of those services where necessary.

The underlying principle is that TfL has well-defined and tested cyber security incident management processes in place, that aim to ensure continuity of essential services in the event of an incident affective systems or services.

4 OT Project Lifecycle

All OT projects and operational systems must undertake cyber security activities and implement cyber security controls throughout both the project lifecycle as well as the operational lifecycle. For the purposes of this standard, it is necessary to manage cyber security throughout the entire OT project lifecycle which consists of four key phases: design, build, operation, and decommissioning. This is referred to as a "secure by design" approach.

4.1 OT Project Lifecycle

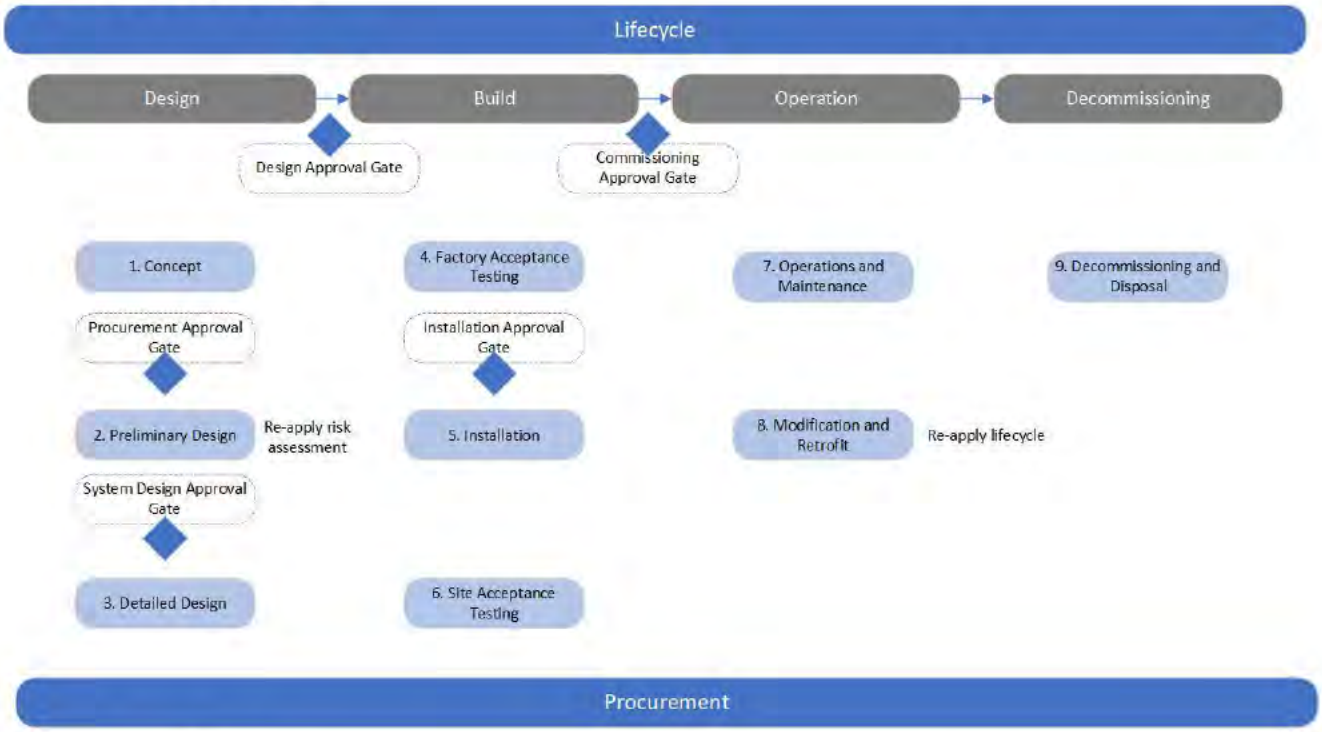


Figure 1 - OT Lifecycle

Implementing security protection measures into OT can be more difficult and costly once systems have been built and deployed. Even more important is that bolting on security measures to either in-service OT, or late in the development cycle of that OT, is often less effective than building them in at the beginning. Dealing with security risks by integrating protection measures into the OT early in its lifecycle is more effective, avoids overruns, is usually less costly and can often be a business enabler.

4.2 Good Practice Principles

To effectively manage the OT lifecycle within the organisation there are five good practice principles which bridge the gap between the lifecycle and cyber security frameworks and bring manageable actions to supporting the lifecycle.

The good practice principles are to:

- Ensure regulatory and security requirements are included in procurement and penalties are flowed down
- Ensure OT systems are secure by design
- Manage security through OT system construction
- Manage operational security
- Managing security risks during decommissioning and disposal.

Further detail for each principle is contained in the supporting guidance document, G1771 Operational Technology Cyber Security – Projects and Upgrades.

4.3 OT Project Lifecycle Requirements

The project must establish and undertake the following activities during the OT project lifecycle:

4.3.1 Concept Phase

Security Awareness Training

4.3.1.1 All staff involved in the procurement, development and deployment of OT assets must receive appropriate cyber security awareness training. Staff directly involved in the cyber security engineering of OT assets must be able to demonstrate competency in this domain.

Risk Assessment:

4.3.1.2 The project must undertake a cyber security risk assessment to assess the cyber security risk of a system and to determine additional cyber security controls above that of the minimum-security baseline requirements established within this standard.

4.3.1.3 Following the risk assessment, the project must develop a cyber security risk treatment plan containing a prioritised list of cyber risks and controls to eliminate, mitigate or contain each risk. This plan must be updated throughout the life of the project and form part of the handover documentation.

4.3.1.4 The risk assessment and ongoing management shall be conducted according to S1770 Operational Technology Cyber Security – Governance.

Threat Modelling:

4.3.1.5 The project must undertake assessment of cyber threats to inform the cyber security risk of a system.

4.3.1.6 This should consider the full range of attacker types, their associated motivations, potential access vectors, attack methodologies and the impacts of any attack on safe operations. MITRE ATT&CK for ICS is a possible tool to support this analysis.

4.3.2 Preliminary Design Phase

Security Requirements:

4.3.2.1 The project must incorporate the minimum cyber-security baselines requirements from this standard into the project requirements. This shall form the basis of the cyber security plan for the project.

4.3.2.2 The project may have to include additional requirements, such as those arising from the risk assessment or aligned to increased controls for safety critical systems into the project requirements.

Preliminary Design:

4.3.2.3 The project must verify and validate that the project cyber security requirements are addressed within the preliminary design.

4.3.2.4 As a minimum, the following documentation shall be produced during the preliminary design phase:

- High Level or Concept Design
- Draft Network specifications and proposed configurations
- Draft interface specifications
- Draft cyber security plan
- High Level Security Architecture.

4.3.2.5 The project shall expect the level of detail in the design and architecture to include all the security controls to be implemented along with an inventory of all the communication flows and interfaces of the OT assets and the system segmentation, in the form of a Security Zones proposal, to demonstrate a planned intent to satisfy all the cyber security requirements.

4.3.2.6 The preliminary design must also demonstrate that functional and operational objectives of the system are capable of being met.

4.3.3 Detailed Design Phase

Detailed Design

4.3.3.1 The project must verify and validate that the project cyber security requirements are addressed within the detailed design.

4.3.3.2 The project must use the preliminary design to undertake the development of a detailed design able to satisfy all the cyber security requirements.

4.3.3.3 The project must adopt appropriate secure coding practices, including, but not limited to OWASP and Top 20 PLC Secure Coding Practices.

4.3.3.4 As a minimum, the following documentation shall be produced:

- Low Level or Detailed Design
- Network specifications and configurations
- Network traffic profile and expected communication paths
- Interface specifications

- Cyber security plan
- Security Architecture, including Zone and Conduit model.

4.3.3.5 The detailed design process must:

- Define, develop, document, and validate the required cyber security design
- Justify interfaces between OT assets assigned to different security Zones and domains of trust
- Confirm that any interfaces within a security Zone do not result in a reduction of the cyber security for assets within the Zone
- Confirm that any interfaces between security Zones do not result in a reduction of the overall cyber security of the Zones
- Confirm that any interfaces between OT assets and external domains of trust do not result in a reduction of the cyber security for the asset or system.

4.3.3.6 Once the detailed design has been established, verification must be performed to ensure that all the cyber security requirements have been met.

4.3.3.7 The verification process must include a review of:

- Any deficiencies in the design that might allow inadvertent, unintended, or unauthorised access or modifications to OT assets that might degrade the safety, reliability, integrity, or functionality during operation.
- Ineffectiveness of safety functions relating to OT assets in the presence of undesired cyber behaviour from connected systems.

4.3.3.8 Any observed deficiencies from the verification process must be corrected by revising either the cyber security requirements or the design to resolve the deficiency. The results of the verifications shall be documented in a design output document, such as the design review report.

Incident Management

4.3.3.9 There must a defined process to effectively manage cyber security events during the project lifecycle with the objective of minimising impacts on the project and maintaining or restoring normal operations.

4.3.3.10 Formal event reporting and escalation procedures must be established.

4.3.3.11 There must be procedures in place to identify cyber security events and respond to them.

Secure Development and Testing Environments

4.3.3.12 The project must review details of development and testing processes including policies, procedures, practices, and technical environments to ensure they are cyber-secure (see 4.3.3.13).

4.3.3.13 The project must confirm the acquisition and handover of secure OT assets which are free of malware, vulnerabilities or weaknesses resulting from insecure product development and/or testing processes.

4.3.3.14 There must be a secure development and testing framework which must:

- Ensure that secure development and testing environments (including tools and development facilities) are established.
- Ensure that secure development and testing processes are established and applied.
- Ensure that all the applicable controls defined in this standard are implemented, providing evidence of their implementation.
- Document standards, coding practices, technical details of the development and testing environments, maintenance plans, secure development and testing methodologies, and product benchmarking against well-defined standards and frameworks.
- Identify countries of origin of the products used and where their assembly, development and testing are undertaken
- Demonstrate quality assurance
- Demonstrate contingency planning for assets during product development and testing
- Ensure that software maintenance plans, including software recovery information, are available during the contract lifecycle and afterwards for maintenance.

Continuous Verification and Validation

4.3.3.15 Each security control of the OT assets must be regularly validated by test or demonstration during development and commissioning to ensure that it does not degrade the following to an unacceptable level:

- Safety
- Functionality
- Performance.

4.3.3.16 Testing of OT assets must be conducted fully and in multiple stages to ensure correctness in the final environment.

4.3.3.17 All verification and validation tests must be documented.

4.3.4 Factory Acceptance Testing Phase

Factory Acceptance Testing

4.3.4.1 The project must ensure that functional testing of the cyber security controls is completed on the system within the constraints of a factory setting.

4.3.4.2 The project must ensure that penetration testing in completed on the system during Factory Acceptance Testing (FAT).

Factory and Site Acceptance Testing Requirements

The following requirements must be met at both the FAT and Site Acceptance Testing (SAT) stages of delivery:

4.3.4.3 The project must receive documentation to confirm that all applicable manufacturer updates and patches have been installed prior to testing.

MAYOR OF LONDON
Transport for London
TfL RESTRICTED

4.3.4.4 The project must receive documentation to confirm that all applicable requirements have been met prior to testing.

4.3.4.5 The project must receive documentation to confirm the absence of vulnerabilities, or the effectiveness of implemented mitigation and containment controls.

4.3.4.6 The project must receive documentation to confirm the absence of malware prior to testing.

4.3.4.7 The project must confirm that the testing is conducted across a fully representative sample of all types of OT assets present in the system throughout the testing period.

4.3.4.8 The project must confirm that the system remains free of malware throughout the testing process.

4.3.4.9 The project must confirm that the system performs as expected in terms of safety, function, and performance under cyber-attack scenarios.

4.3.4.10 The project must specify that penetration tests are conducted and reported according to NIST Special Publication 800-115 (SP 800-115). Furthermore, the penetration tests must be conducted by an independent specialist testing company.

4.3.4.11 The project must receive updated cyber security risk assessments based on the findings of the completed penetration test and implement or update risk treatment plans where necessary.

4.3.4.12 The penetration test scenarios must be defined by the independent specialist testing company, with input from the project, and agreed with the project in advance. Suppliers may be involved in the development of test scenarios.

4.3.5 Installation Phase

Training

4.3.5.1 The project must ensure that cyber security training is undertaken by operational and maintenance staff relating to the cyber security requirements, controls, and deliverables of the system.

Installation

4.3.5.2 The installation must be planned and conducted in accordance with the overall project cyber security plan.

4.3.5.3 The project must ensure that OT assets are protected during installation activities and that the Installation Work Plan highlights specific cyber security risks of the installation process, with the actions taken to reduce them to acceptable levels.

4.3.5.4 The project must ensure there is a plan which identifies the actions required to return OT assets to a state within the tolerable cyber security risks levels, should they be exposed to unplanned risk during the installation process.

4.3.5.5 Before installation, the project must ensure that the security of any tools has been assessed and confirmed as secure, free from malware and containing only essential software to support the installation.

4.3.5.6 After installation, the project must ensure that the tools have been assessed and confirmed clean to prevent the leak of the confidential data relating TfL or the installed system.

4.3.6 Site Acceptance Testing Phase

Site Acceptance Testing

4.3.6.1 The project must ensure that functional testing of the cyber security controls is completed on the system within the constraints of a non-operational site setting.

4.3.6.2 The project must undertake penetration testing of the system at SAT.

4.3.6.3 The project must undertake necessary remediation activities as a result of SAT.

4.3.7 Operations and Maintenance Phase

Documentation

4.3.7.1 The project must receive documentation covering the design of the cyber security controls and their ongoing operation and maintenance.

4.3.7.2 As a minimum, the following documentation is to be provided for handover:

- Operational manuals, processes and procedures
- Network specifications and configurations
- Baseline network traffic plan
- Cyber security plans
- Asset Register
- High Level Design (HLD) or Concept Design document
- Low Level Design (LLD) or Detailed Design Document.

Handover into Operation

4.3.7.3 The project must receive documentation to confirm that all the cyber security controls have been verified and validated as functional at handover.

4.3.7.4 The project must receive documentation to confirm that, where possible, identified risks and remediations have been closed out and that appropriate mitigating controls have been implemented where this has not been possible.

Training

4.3.7.5 The System Owner and Lead Maintainer must receive a comprehensive training plan encompassing the entire cyber security scope, developed security plans as well as the technical features and implementation details of the solutions developed/deployed during the project lifecycle.

4.3.8 Modifications and Retrofit Phase

Operation and Maintenance

Prior to any modification of an OT asset, a cyber security risk assessment must be conducted to confirm that any temporarily disabled security features will not significantly impact the overall security posture of the OT asset during modification.

4.3.8.1 For any OT asset modification, the overall security posture of the current cyber security plan should be considered to ensure that the maintenance of the system provides assurance that implemented controls remain in place, and continue to operate correctly, and that the plan itself continues to remain effective.

Secure Supply Chain

4.3.8.2 The project must ensure that secure supply chain requirements apply to both hardware and software assets.

4.3.8.3 There must be an ongoing process to protect the supply chain for OT assets. This process must contain adequate plans, policies, procedures, and registers to continually demonstrate to the project and system owner that the supply chain remains secure.

4.3.8.4 The secure supply chain must be used throughout the project lifecycle.

4.3.8.5 There must be controls in place to protect the systems during their physical or logical transport ensuring that the assets are not vulnerable to subversion, including malicious code insertion, counterfeit insertion, and tampering.

4.3.8.6 The secure supply chain process must be extended to third party products which are incorporated into the system.

4.3.8.7 The secure supply chain process must address and continually demonstrate the following during the project or contract lifecycle:

- Chain of custody practises and updated documentation.
- Inventory management including the location and protection of physical and logical assets including spare parts.
- Information protection
- Secure digital products delivery
- Trusted channels and controls to ship assets including tamper-proof packaging
- Controls to detect unauthorised access and/or alteration throughout the delivery process
- Cascading of these cyber security requirements to the entire supply chain
- Collection and preservation of evidence demonstrating security of the supply chain.

4.3.9 Decommissioning and Disposal Phase

Disposal and Decommissioning

The project must have procedures in place to address decommissioning and secure disposal of OT assets (including media) in a controlled manner, to avoid disruption to interfacing OT assets and disclosure of sensitive information.

The project must assess and document the effect of replacing or removing an existing OT asset and/or security function. The scope of this assessment must include interfacing OT assets.

4.4 The Purdue model and Secure OT Design

Sections 4.4 to 4.8 of the guidance document (G1771) provide knowledge and understanding which support the good practice principles in Section 4.2 and the OT Project lifecycle requirements in Section 4.3.

5 Protecting against cyber attack

The following controls will contribute to protecting TfL's OT against cyber-attack and establish the minimum baseline of cyber security measures for all new projects and upgrades to existing systems. Safety critical and service critical systems must also be risk assessed and are expected to require additional controls above the minimum baseline, for which suggestions are shown in the notes.

5.1 Identity and access control

TfL must assure good management and maintenance of identity and access control for the networks and information systems supporting TfL services.

The requirement is that the project will have to develop a list of all users (humans, software processes and devices) and to determine for each control system component the required level of Identity and Access Control (IAC) protection.

Access control is the method of controlling who or what entities can access premises and systems, as well as the type and level of access that is permitted. There are three key aspects associated with access control:

- account administration
- authentication
- authorisation.

All three aspects shall work together to establish a sound and secure access control strategy. Account administration is the method associated with granting and revoking access accounts and maintaining the permissions and privileges provided under these accounts to access specific resources and functions on the physical premises, network, or system. Access accounts should be function or role-based and may be defined for individuals, groups of individuals functioning as a crew or for devices providing a function.

The detailed requirements are aligned to the headings below to group requirements under common functions and to support traceability to the NIS regulations where required.

5.1.1 Account administration

As an organisation, TfL must ensure, on an ongoing basis, that only appropriate individuals or entities have accounts that allow access and that these accounts provide appropriate access privileges.

The project must ensure that any system can support the following minimum baseline requirements:

5.1.1.1 Access shall be granted, changed, or terminated on the authority of an appropriate manager or system owner.

MAYOR OF LONDON
Transport for London
TfL RESTRICTED

5.1.1.2 A record shall be maintained of all access accounts, including details of the individual(s) and devices authorised to use the account, their permissions, and the authorising manager.

5.1.1.3 Access accounts shall be suspended or removed as soon as they are no longer needed, for example in the event of a job change. 3rd parties engaged on the support and maintenance of systems are required to notify TfL of Joiners, Movers and Leavers.

5.1.1.4 All established access accounts shall be reviewed three-monthly to ensure that the accounts only provide the minimum required permissions.

5.1.1.5 The use of default accounts and passwords is forbidden.

5.1.1.6 Passwords for access accounts shall be changed from default or test credentials before the system is handed into operation.

5.1.1.7 Periodic reviews of compliance, minimum six-monthly, to the account administration policy and process should be performed.

Note: For safety critical and service critical systems the following additional requirements shall apply:

5.1.1.8 Unified account management (for example, an Active Directory service supporting multiple systems within a security Zone)

5.1.2 Authentication

As an organisation, TfL must positively identify network users, hosts, applications, services, and resources for computerised transaction so that they can be given the rights and responsibilities associated with the accounts they have been granted under account administration.

The project must ensure that any system can support the following minimum baseline requirements:

5.1.2.1 All users must be authenticated before using an application or system.

5.1.2.2 Anonymous authentication shall not be permitted.

5.1.2.3 There shall be no hard-coded credentials in the system.

5.1.2.4 Root accounts shall not be used as main credentials.

5.1.2.5 All default credentials must have been changed by FAT.

5.1.2.6 All system administrator access accounts and application configuration access accounts shall have strong authentication practices (such as requiring strong passwords or Multi Factor Authentication (MFA).

5.1.2.7 There shall be no use of SMS for MFA (alternatives are one-time passcodes from an app like Google Authenticator or hardware MFA).

Where this is not technologically achievable, possible compensating controls could include separate physical or electronic entrance control technologies or administrative practices, such as a two-person rule.

In large scale or distributed systems, the use of a centralised access control system, such as LDAP or Radius, should be considered.

5.1.2.8 After 3 failed login attempts by a local or remote user, the system should disable the associated access account for 3 hours. There may need to be exceptions for local accounts on systems where constant access is required, such as Human Machine Interfaces (HMIs) in control rooms.

5.1.2.9 After 30 minutes of inactivity, a local or remote user should be required to re-authenticate before the user can re-access the system. There may need to be exceptions for local accounts on systems where constant access is required, such as HMIs in control rooms.

5.1.2.10 The system shall not allow multiple concurrent logins.

5.1.2.11 The system shall not allow applications to retain authentication data between sessions.

5.1.2.12 All access attempts to critical systems should be recorded and retained in a log file for a minimum period of three months.

5.1.2.13 Log Files should be reviewed for successful and failed access attempts as well as unusual or unexpected activity such as out of hours access or attempts to access the system by unauthorised users.

5.1.2.14 Systems should employ an authentication scheme (such as X.509) for task-to-task communication between applications and devices.

Note:	For safety critical and service critical systems the following additional requirements shall apply:
5.1.2.15	Multifactor authentication for untrusted networks.
5.1.2.16	Multifactor authentication for all networks.

5.1.3 Authorisation

As an organisation, TfL must grant access privileges to resources after successful authentication of the user and identification of their associated access account. The privileges granted are determined by the account configuration set up during the account administration step in the business process.

The project must ensure that any system can support the following minimum baseline requirements:

5.1.3.1 There must be clearly documented rules that define the privileges authorised for access accounts which are aligned to the job roles for the system. These rules must follow the principles of least privilege.

5.1.3.2 The system must apply these rules to all users upon authentication.

5.1.3.3 Access accounts must be role based to manage access to appropriate information or systems for that user's role.

5.1.3.4 Safety implications shall be considered when defining roles.

Note:	For safety critical and service critical systems the following additional requirements shall apply:
5.1.3.5	Unique identification and authorisation.

5.1.3.6 Hardware security for software process identity credentials.

5.1.4 Passwords

As an organisation, TfL must ensure that for control systems utilising password-based authentication, the control system shall provide the capability to enforce configurable password strength based on minimum length and variety of character types.

The project must ensure that any system can support the following minimum baseline requirements:

If an OT system does not have the capabilities to meet all the password requirements, a concession must be raised.

5.1.4.1 The system shall provide a configurable password management facility to allow passwords to be selected according to the requirements in 5.1.4.2.

5.1.4.2 Passwords must meet the following requirements:

- Minimum 13 characters long when set by a human.
- Minimum 13 characters long minimum when set by a system/service.
- The system must support a password of at least 64 characters maximum length.
- All ASCII characters (including space) shall be supported for passwords.
- The password shall not be truncated when processed.
- The chosen password shall be checked with known password dictionaries.
- The system shall allow the number of password attempts before lockout to be set (5.1.2.8 refers).
- The system shall deny the repeated use or recycling of the last five passwords.
- There shall be no complexity requirements for passwords.
- There shall be no password expiration period.
- There shall be no password hints.
- There shall be no knowledge-based authentication (e.g. who was your best friend in high school?).

5.1.4.3 Passwords shall not be stored, electronically or hard copy, in plain text. The exception to this requirement is the sharing of an initial or recovery password with an authorised user, which must be in a separate communication to the user identification.

5.1.4.4 Copies of root, administrator, and system account details, retained for emergency use, must be stored separately from the system and in a secure storage.

Note: For safety critical and service critical systems the following additional requirements shall apply:

5.1.4.5 Password generation and lifetime restrictions for human users

5.1.4.6 Password lifetime restrictions for all users

5.1.5 Wireless Access Management

As an organisation, TfL must ensure that the control system provides the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.

The project must ensure that any system can support the following minimum baseline requirements:

5.1.5.1 The control system shall provide the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.

5.1.5.2 Wireless networks shall have MAC Address filtering enabled.

5.1.5.3 The system shall provide the capability to authorise, monitor and enforce usage restrictions for wireless connectivity to the control system.

5.1.5.4 Wireless systems shall employ a key management system.

5.1.5.5 Wireless encryption requirements are contained Section 5.5.5 (Encryption).

5.1.5.6 Wireless devices shall be protected with security controls, such as access control and encryption, to protect the devices from unauthorised access, modification, or use.

5.1.5.7 Where Public Key Infrastructure (PKI) is utilised, the control system shall provide the capability to operate a PKI according to commonly accepted best practices or obtain public key certificates from an existing PKI.

Requirements 5.1.5.8, 5.1.5.9, 5.1.5.10 and 5.1.5.11 are only applicable to systems that provide open public WIFI networks at Stations and on passenger trains or trams.

5.1.5.8 The system shall be designed so that open public WIFI networks can be disabled within 15 minutes.

5.1.5.9 The system shall be designed so that disabling open public WIFI networks does not affect the operational railway system.

5.1.5.10 The project shall document and test a process to disable open public WIFI networks within 15 minutes of being requested.

5.1.5.11 The project shall document and test a process to reenable open public WIFI networks

Note: For safety critical and service critical systems the following additional requirements shall apply:

5.1.5.10 Hardware security for public key authentication

5.1.6 User Change Management and Access Review

As an organisation, TfL must ensure they are able to track joiners, movers and leavers in order to ensure that each individual user is only granted minimum required access rights for their role, that these rights are reviewed when they change role and revoked on leaving TfL.

It is essential that access to any OT system which supports the delivery of TfL services is authorised by the system owner or a delegated deputy (Section 5.1.1.1 refers).

System owners should conduct a regular review of user access rights for the system(s) they are responsible for and ensure those which are no longer required are revoked (Sections 5.1.1.3 and 5.1.1.4 refer).

Projects must provide the capabilities within the systems they are delivering to support these user change management and access review activities through the following minimum baseline requirements:

5.1.6.1 The system shall provide the capability to uniquely identify and authenticate all human users.

5.1.6.2 The system shall provide the capability to uniquely identify and authenticate all non-human users.

5.1.6.3 This identification and authentication shall be enforced on all interfaces which provide access to the control system to support the verification of the principle of least privilege.

5.1.6.4 The system shall provide the capability to support the management of all accounts by authorised users, including adding, activating, modifying, disabling, and removing accounts.

5.1.6.5 The system shall provide the capability to support the management of identifiers by user, group, role, or control system interface.

5.1.6.6 The system shall provide the capability to:

- change all default authenticators upon control system installation.
- change/refresh all authenticators; and
- protect all authenticators from unauthorised disclosure and modification when stored and transmitted.

5.1.7 Monitor Access

As an organisation, TfL must provide the capability to log and monitor all user access to any OT system, which will form an integral element of system monitoring.

The project must ensure that any system can support the following minimum baseline requirements:

5.1.7.1 The system shall provide the capability to obscure feedback on authentication information during the authentication process. (For example, responding to a failed login attempt with a “login failed” message rather than “your password was incorrect” which shows an attacker they have used a valid user ID).

5.1.7.2 The system shall provide the capability to enforce a configurable number, currently three (Section 5.1.2.8 refers), of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period, which is recommended to be set at thirty minutes.

5.1.7.3 The system shall provide the capability to deny access for three hours or until unlocked by an administrator when the consecutive invalid access attempts limit has been exceeded (Section 5.1.2.8 refers).

5.1.7.4 The system shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorised personnel.

5.1.7.5 The system shall provide the capability to enforce authorisations assigned to all users (humans, software processes and devices) for controlling use of the system to support Segregation of duties and least privilege.

5.1.7.6 The system shall provide the capability for an authorised user or role to define and modify the mapping of permissions to roles for all human users, software processes and devices.

5.1.7.7 The system shall provide the capability to automatically enforce configurable usage restrictions that include:

- preventing the use of portable and mobile devices
- restricting code and data transfer to/from authorised portable and mobile devices.

5.1.7.8 The system shall provide the capability to log, including but not limited to:

- Failed log in attempts
- Automatic account reset
- Administrative account reset
- Successful logins out of normal working patterns
- Password changes
- Permission changes
- Failed attempts to connect unauthorised portable and mobile devices
- Connection of authorised portable and mobile devices.

5.1.7.9 The system shall provide the capability to forward user logging securely to a central log collector (Section 6 refers).

5.2 Data Security

TfL must protect data which is stored or transmitted electronically from actions such as unauthorised access, modification or deletion that may cause an adverse impact on essential functions.

This protection must be underpinned by a good understanding of the data that is important to the delivery of the TfL services, where it is stored, where it travels, and how unavailability or unauthorised access, modification or deletion would impact the service. This also applies to any third parties storing or accessing data important to the delivery of TfL services.

5.2.1 Identify and Understand Critical Data (Information and Documents)

As an organisation, TfL must ensure that for each OT system, there is a record of the location, type, quantity, and quality of data important to the delivery of TfL services. In addition, this record must include the context, limitations and dependencies of the data that is critical to TfL services.

Much of the information about the OT system may be stored electronically or in hardcopy outside the system and is not protected by OT authorisation controls. Unauthorised access and use of this information are a threat to OT security and this information needs to be appropriately controlled and managed.

The project must provide the following minimum baseline requirements:

5.2.1.1 A document management process shall be developed and maintained for OT information which supports the system.

5.2.1.2 Information classification levels, commensurate with S1782 Information Security Classification, shall be defined for access and control, including sharing, copying, transmitting, and distributing of OT information.

5.2.1.3 All logical assets within the scope of the project (including, but not limited to, system design information, vulnerability assessments and network diagrams) shall be classified to indicate the protection required commensurate with the consequence of compromise. (S1782 – Information Security Classification refers).

5.2.1.4 Policies and procedures, commensurate with S1782 Information Security Classification, should be developed for retention, physical and integrity protection, destruction, and disposal of all assets based on their classification, including written and electronic records, equipment and other media containing information, with consideration for legal or regulatory requirements.

5.2.1.5 Measures shall be employed to ensure long-term records can be retrieved. This could include converting the data to a newer format or retaining older equipment that can read the data.

5.2.1.6 Information that requires special control or handling shall be reviewed on a periodic, at least annual, basis to validate that special handling is still required.

5.2.1.7 Annual reviews of compliance to S1782 Information Security Classification shall be performed.

5.2.2 Understand Data Links

As an organisation, TfL must ensure that for each OT system, there is a documented and up to date understanding of the data links used to transmit data that is critical or important to the delivery of TfL services.

The project must provide the following minimum baseline requirements:

5.2.2.1 A documented record of all the data links that transfer data into or out of the system.

5.2.2.2 The record must include the context, limitations and dependencies of the data links that are critical to TfL services.

5.2.2.3 The record shall support and inform the capability to protect the integrity of transmitted information (Section 5.5.2 refers).

5.2.3 Identify Mobile Devices and Portable Media

As an organisation, TfL must ensure that all mobile devices and media that may hold data important to the delivery of the TfL services and are used to support the OT system must be identified and recorded.

Mobile devices include but is not limited to laptop computers and handheld programmers. Media assets include removable media and devices such as floppy disks, CDs, DVDs, and USB memory sticks, as well as printed reports and documents.

If an adversary gains access to backup media associated with an OT system, it could provide valuable data for launching an attack. Recovering an authentication file from the backups might allow an adversary to run password cracking tools and extract usable passwords. In addition, the backups typically contain machine names, IP addresses, software version numbers, usernames, and other data useful in planning an attack.

The project must provide the following minimum baseline requirements:

5.2.3.1 The use of any unauthorised mobile device or portable media on any node that is part of or connected to the OT system shall not be permitted in order to prevent the introduction of malware or the inadvertent loss or theft of data.

5.2.3.2 Systems shall only use removable media and mobile devices where absolutely necessary and must undergo business justification and further risk assessment to provide justification for all enabled USB ports, CD/DVD drives and other removable media devices.

5.2.3.3 Where the use of a mobile device or portable media is permitted, this must be a dedicated device which is subject to an equivalent level of protective controls to the OT system that it is used to support.

5.2.3.4 There shall be a documented process to verify that a mobile device is free from malware before it is connected to the system (Section 5.7.1 refers).

5.2.3.5 A documented record of all authorised mobile devices and portable media which are associated with the system must be maintained/created.

5.2.3.6 The number of authorised removable media and mobile devices shall be kept to the absolute minimum required for system operation.

5.2.3.7 Mobile devices and portable media that will be transported between physically secure locations is to employ data at rest encryption.

5.2.3.8 Where the use of removable media is authorised and the system supports it, software can be used to enforce removable media processes.

5.2.4 Manage Data Holdings

As an organisation, TfL must ensure that data holdings relating to OT are managed throughout the life of the system.

The project must provide or ensure the following minimum baseline requirements:

5.2.4.1 A documented record of data holdings relating to the system which will include, but not be limited to, design documentation, operational data, system logs and backups.

MAYOR OF LONDON
Transport for London
TfL RESTRICTED

5.2.4.2 The system shall provide the capability to review and then remove or minimise unnecessary copies or unneeded historic data.

5.2.4.3 Data retention must be aligned to regulation, system operating requirements and security monitoring requirements. For example, if system logs are ingested into a centralised logging system, they do not need to be retained in perpetuity on the system, but only for local fault finding or recovery purposes, which would require up to a months' worth of data.

5.3 Personnel Security

TfL must closely manage privileged user access to networks and information systems supporting the TfL services.

Personnel security has three related aspects. From an organisational HR perspective, it involves looking at new and current personnel to determine if they will maintain the OT security for the organisation. For new personnel, the personnel security process evaluates them prior to their entry into the organisation making sure they demonstrate behaviours consistent with their future security responsibility. For current personnel, the personnel security process establishes that they continue to demonstrate behaviour consistent with their current security responsibilities.

Personnel security requirements are also driven by concerns about training, approved staff, awareness of the system, awareness of safety and in some instances malicious activity (generally referred to as Insider Threats). For more information on Insider Threats refer to G1134: Personnel Security – Insider Threat.

From a project perspective, the approach is ensuring that the system has the required capabilities to support the minimum baseline controls for personnel security and builds on the baseline identity and access control requirements in Section 5.1.

5.3.1 Privileged User Access

TfL must ensure that individuals who require privileged levels of user access receive additional validation and authentication.

The project must provide the following minimum baseline requirements:

5.3.1.1 Privileged access shall be granted, changed, or terminated on the authority of an appropriate senior manager or system owner.

5.3.1.2 Privileged access accounts should be dedicated to a specific function and must not be used for general administrative tasks.

5.3.1.3 Privileged access accounts must use MFA.

5.3.1.4 A non-privileged user must not be able to gain privileged access rights without proper authorisation and such authorisation should only be temporary to support an urgent business need.

5.3.1.5 On all interfaces, the system shall provide the capability to enforce authorisations assigned to all users (humans, software processes and devices) for controlling use of the system to support Segregation of duties and least privilege.

5.3.1.6 The system shall provide the capability for an authorised user or role to define and modify the mapping of permissions to roles for all human users.

5.3.2 User Management

TfL must ensure that the identities of the individuals, whether employees or partners, with privileged access to networks and information systems to support the TfL services systems are known and managed.

The project must provide the following minimum baseline requirements:

5.3.2.1 A record shall be maintained of all privileged access accounts, including details of the individual(s) and devices authorised to use the account, their permissions, and the authorising manager.

5.3.2.2 Privileged access accounts shall be suspended or removed immediately when they are no longer needed, for example in the event of a job change.

5.3.2.3 The system shall provide the capability to automatically enforce configurable usage restrictions for users that include:

- preventing the use of portable and mobile devices
- requiring context specific authorisation; and
- restricting code and data transfer to/from portable and mobile devices.

Note: For safety critical and service critical systems the following additional requirements shall apply:

5.3.2.4 Supervisor override

5.3.2.5 Hardware security for public key authentication.

5.3.3 Role Based Access

TfL should ensure that privileged users are granted only specific privileged permissions which are essential to their business role or function.

The project must provide the following minimum baseline requirements:

5.3.3.1 Duties should be segregated amongst personnel to maintain appropriate checks and balances, so that no single individual has total control over actions that change the functional operation of the OT.

5.3.3.2 Personnel should be assessed for the critical positions controlling and maintaining the OT.

5.3.4 Privileged Access Review

TfL must conduct a regular review and validation of activity by privileged and standard users to identify any unauthorised or unusual activities.

The project must provide the following minimum baseline requirements:

5.3.4.1 All established privileged access accounts shall be reviewed monthly to ensure that the accounts only provide the minimum required permissions and remain a valid requirement for operating the system.

5.3.4.2 The system shall provide the capability to generate audit records relevant to privileged account security for the following categories:

- access control

- request errors
- operating system events
- system events
- configuration changes
- potential reconnaissance activity and audit log events.

5.3.4.3 Individual audit records shall include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result.

5.3.4.4 The system shall allocate sufficient audit record storage capacity for log management and system configuration. This shall be to a minimum of one year's worth of records.

5.3.4.5 The system shall provide timestamps for use in audit record generation.

Note: For safety critical and service critical systems the following additional requirements shall apply:

5.3.4.6 Supervisor override

5.3.4.7 Hardware security for public key authentication.

5.4 Physical Security

TfL must ensure that physical security arrangements compliment OT cyber security and protect the OT supporting the TfL services from direct attack.

This will create a secure environment for the protection of OT assets.

This section should be read in conjunction with established physical security standards (Listed or linked in Section 13) and in consultation with the physical security team. The intention is to ensure that physical and cyber security arrangements are complementary and considered properly at each stage of design, development and delivery. This section is not intended to replace established physical security standards, but rather to highlight to TfL staff and partners where particular physical security considerations are relevant to OT systems.

Surveillance and security systems, in particular CCTV, access control systems and intruder detection systems shall comply with S1147 Surveillance and Security Systems.

An asset is any physical or logical object owned by, or operated by, TfL having either a perceived or actual value to the organisation for delivery of TfL services. OT assets are those assets that are a part of the OT, either physical or cyber or that can affect the operation of the OT.

IT assets used in support of or as part of OT systems shall comply with S1747 Physical Security of IT Equipment.

Physical security measures ensure that all assets, specifically those related to the OT of an organisation, are protected physically from unauthorised access, loss, damage, misuse, and the like. Environmental security measures ensure that the assets of an organisation are protected against environmental conditions that would make them unusable or damage the information they contain.

Physical and environmental security measures should be designed to complement the cyber security measures taken to protect assets that are part of the OT and coordinated with the physical security of the remainder of the infrastructure.

It is important to include all systems in the scope and not just limit the effort to traditional computer room facilities and equipment rooms. Practical engineering judgment should be used to balance the risks when determining physical security procedures.

Physical segmentation is a key security countermeasure designed to compartmentalise devices into security Zones where identified security practices are employed to achieve the desired target security level.

The physical protection of the cyber components and data associated with the system must be addressed as part of the overall security of a system. Security at many OT facilities is closely tied to site safety. A primary goal is to keep people out of hazardous situations without preventing them from doing their job or carrying out emergency procedures. Physical security controls are any physical measures, either active or passive, that limit physical access to any information assets in the OT environment.

These measures are employed to prevent many types of undesirable effects, including:

- Unauthorised physical access to sensitive locations
- Physical modification, manipulation, theft or other removal, or destruction of existing systems, infrastructure, communications interfaces, personnel, or physical locations
- Unauthorised observation of sensitive informational assets through visual observation, note taking, photographs, or other means
- Prevention of unauthorised introduction of new systems, infrastructure, communications interfaces, or other hardware
- Prevention of unauthorised introduction of devices intentionally designed to cause hardware manipulation, communications eavesdropping, or other harmful impact.

The project must provide the following minimum baseline requirements:

5.4.1.1 Security procedures that address the physical security in the protection of assets shall be established for the system

5.4.1.2 At least one physical security perimeter shall be established to provide barriers to unauthorised access to protected assets. Critical components and systems must have at least two physical perimeters.

5.4.1.3 There must be entry controls at each physical barrier or boundary.

5.4.1.4 There shall be an auditable record of access to equipment via a security barrier or boundary.

5.4.1.5 All connections under the control of the project shall be adequately protected from tampering or damage.

MAYOR OF LONDON
Transport for London
TfL RESTRICTED

5.4.1.6 Arrangements must be established to protect assets against environmental damage from threats such as fire, water, smoke, dust, radiation, corrosion, and impact.

5.4.1.7 Maintenance procedures must be established for all equipment assets, including auxiliary environmental equipment, to ensure proper operation through correct maintenance.

5.4.1.8 Procedures shall be established for monitoring and alarming when physical or environmental security is compromised.

5.4.1.9 Procedures should be established and audited with respect to the addition, removal, and disposal of all assets.

5.4.1.10 Procedures shall be established to ensure the protection of critical components during the interruption of operations, for example, due to fire, water ingress, security breach, interruption, natural or any other type of disaster.

5.5 Network Security

TfL must ensure that the transit of data important or critical to the delivery of TfL services is protected. This includes the transfer of data to third parties.

5.5.1 Data Transfer

The project must ensure that:

5.5.1.1 All Conduits for data transfer have been identified according to Section 5.2.2.

5.5.1.2 Conduits shall be designed to protect the data they are transferring. Options to protect the data include, but are not limited to:

- Encryption (See Section 5.5.5)
- Secure Tunnelling, such as VPNs (See Section 5.5.6)
- Data Diodes
- Inbound and outbound boundary (firewall) rules.

5.5.2 Data Protection

TfL must ensure that the system has the capability to protect the integrity of transmitted information.

The project must provide the following minimum baseline requirements:

5.5.2.1 The system shall provide the capability to protect the confidentiality of information for which explicit read authorisation is supported, whether at rest or in transit.

The project should pay particular attention to the information confidentiality relating to portable and mobile devices (for example engineering laptops and USB sticks).

5.5.2.2 Authentication information, such as passwords, should be considered confidential, and never be sent in a readable format. The exception to this requirement is the sharing of an initial or recovery password with an authorised user, which must be in a separate communication to the user identification.

5.5.2.3 The system shall provide the capability to protect the confidentiality of information at rest.

5.5.2.4 Communications over untrusted or open networks shall be encrypted (See Section 5.5.5 Encryption for details).

5.5.2.5 The system shall provide the capability to protect the confidentiality of remote access sessions traversing an untrusted network.

Note: Encryption is a common mechanism for ensuring information confidentiality.

5.5.3 Single Points of Failure

TfL must ensure that the system has been designed to eliminate single points of failure where possible.

The project must deliver the following minimum baseline requirements:

5.5.3.1 As part of the design process, the project must identify single points where, due to failure, there is a significant risk of impact on the delivery of the TfL services.

5.5.3.2 Where possible, these single points of failure should be eliminated during the design stages, but if this is not achievable, this should be recorded in the project risk register and incorporated into any response plans for the system.

5.5.4 Resilient Communications

TfL must ensure there are alternative communication paths where there is a significant risk of impact on the delivery of TfL services if a primary communication path is lost or interrupted.

The project must provide the following minimum baseline requirements:

5.5.4.1 As part of the design process, the project must identify communication paths where, due to failure, there is a significant risk of impact on the delivery of the TfL services.

5.5.4.2 The project should incorporate alternative communication paths to eliminate the risk to service delivery in the primary path is lost or interrupted. If an alternative path cannot be found, this should be recorded in the project risk register and incorporated into any response plans for the system.

5.5.5 Encryption

TfL must ensure that the system has capability to protect the integrity of transmitted information.

This section provides the specific requirements for different methods of encryption, but it should also be noted that depending on the location or design of the system in question, alternative controls could be adopted.

The selected encryption method must provide a commensurate level of protection for the data, both at rest and in transit. This protection must be in line with the impact on TfL services if the data is compromised and will most likely be informed by a risk or impact assessment.

Depending on the type of encryption, the project must adopt the following minimum baseline requirements:

5.5.5.1 For Private Key Encryption (Symmetric Key Cipher), a minimum of AES-256 must be used.

5.5.5.2 For stream ciphers, RC4 and algorithms derived from that shall not be used. AES may be used in a cryptographic mode that allows streaming provided that the key is changed in accordance with the limitations of the cryptographic mode chosen. Keys for streaming cipher modes of operation must only be used for one stream and shall not be reused.

5.5.5.3 The Electronic Codebook (ECB) and Cypher Block Chaining (CBC) block cipher mode of operation must not be used.

5.5.5.4 For key exchange, the DH (Diffie-Hellmann) algorithm must be used with a key length of at least 3072-bit (Group 15). Ephemeral Diffie-Hellmann is preferred.

5.5.5.5 For Public Key Infrastructure (Asymmetric Key Ciphers) encryption, the RSA algorithm with a key length of at least 3072-bit must be used.

5.5.5.6 For Public Key Infrastructure (Asymmetric Key Ciphers) authentication, RSA or DSA algorithms with a key length of at least 3072-bit must be used.

> DSA was originally designed for digital signatures and not for general encryption, although it can be used for general encryption purposes. NIST is trying to deprecate DSA in favour of Elliptic-Curve DSA (ECDSA) and Edwards Curve DSA (EdDSA).
>
> Consideration should be given to Elliptic Curve Cryptography (ECC) instead of RSA, such as Elliptic Curve Diffie Hellmann, since for a given approved curve, the key length is roughly halved to get the same strength of encryption.

5.5.5.7 For data hashing, SHA-256 must be used as minimum. SHA3 shall also be allowed as well as SHA2, with more than 256 bits (FIPS 202).

5.5.5.8 For file integrity checking, SHA-2 must be used as a minimum. SHA3 shall also be allowed as well as SHA2, with more than 256 bits (FIPS 202).

5.5.5.9 For 802.11-based infrastructure, WPA2 Enterprise with AES CCMP encryption and EAP-TLS 1.2 must be used as a minimum.

5.5.5.10 All encryption keys must be changed from their default value before use.

5.5.5.11 All encryption keys must be randomly generated, not human-specified; except for file-level encryption passwords specified by individual users.

5.5.5.12 Cryptographically Secure Pseudorandom Number Generators (CSPRNGs) must be used to generate encryption keys and the following CSPRNGs should be used where possible:

- RNGCryptoServiceProvider, CryptGenRandom, FIPSGenRandom or RtlGenRandom (Microsoft Windows XP Service Pack 3 or later only).
- /dev/random, /dev/urandom or /dev/arandom (preferred) (*nix-based systems).
- Any other Evaluation Assurance Level (EAL) 4+ accredited CSPRNGs.
- Any other Federal Information Processing Standard (FIPS) 186-2 compliant CSPRNGs.

5.5.5.13 CSPRNGs based on the following functions are deemed insecure and must not be used:

- Rand()
- Math.Random()

5.5.5.14 Symmetric and Private keys must be stored securely at rest using PKCS#11 or PKCS#12.

5.5.5.15 Encryption hardware should be certified to FIPS 140-2 (tamper evident) as a minimum.

5.5.5.16 Encryption hardware should be protected from physical tampering and uncontrolled electronic connections.

Cryptography also introduces key management issues since robust security policies require periodic key changes. This process becomes more difficult as the geographic size of the OT increases, with extensive OT systems being the most severe example. As site visits to change keys can be costly and slow, it is useful to be able to change keys remotely.

Note: For safety critical and service critical systems the following additional requirements shall apply:

5.5.5.17 Cryptographic integrity protection.

5.5.6 Virtual Private Networks (VPN)

TfL must ensure that any VPN used to encrypt communications is configured securely.

The project must meet the following minimum baseline requirements:

5.5.6.1 When a VPN is implemented, a solution which uses one of the following protocols must be used:

- Internet Protocol Security (IPsec)
- Transport Layer Security (TLS).

5.5.6.2 For remote access connections, the VPN shall include a logical break point (jump server) at an OT De-Militarised Zone (DMZ) to allow the link to be monitored.

5.5.6.3 The project must ensure that VPN devices used to protect systems are thoroughly tested to verify that the VPN technology is compatible with the application or system and that implementation of the VPN devices does not unacceptably affect network traffic characteristics.

5.5.7 Backups

TfL must ensure that there are backups of the data required to restore systems to normal operational capability (See also Section 7.2).

The project must meet the following minimum baseline requirements:

5.5.7.1 The project must ensure that the system can provide suitable, secured backups of the data (systems, software, licenses, configurations, data, and other relevant information) required to allow the TfL services to operate or to restore the TfL

services to an operational state within agreed recovery objectives (Section 7.1.1 refers).

Note: Automated backups are recommended to ensure that all required files are captured with reduced operator overhead.

5.5.7.2 The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be supported by the system without affecting normal operations.

5.5.7.3 Although not usually required for system recovery, information required for post-incident forensic activity (for example, audit logs) should be specifically included in the backup.

5.5.7.4 Where a backup contains confidential information, encryption should be considered where this will not affect any recovery operations, or the backup should be secured in a suitable lockable storage or safe.

5.5.7.5 The system shall provide the capability for backups to be extracted and stored securely in a separate location.

5.5.7.6 Full-bit images shall be recorded as configuration baselines for operational systems and assets. These images must be stored securely.

5.5.7.7 The system shall provide the capability to verify the reliability of backup mechanisms, including the capability to conduct routine tests to ensure the backup process is functioning correctly and that the backups are usable.

5.5.7.8 The backups shall be accessible if an extreme event occurs.

5.6 System Security

TfL must ensure that security is designed into the network and information systems that support the delivery of TfL services from the outset.

The project should adopt secure design principles to minimise the attack surface and ensure that the delivery of the TfL services should not be impacted by the exploitation of any single vulnerability.

5.6.1 Secure by Design

TfL must employ appropriate expertise to design secure networks and information systems supporting the TfL services.

The project must meet the following minimum baseline requirements:

5.6.1.1 The system shall provide the capability to protect the integrity of transmitted information (Section 5.5 refers).

5.6.1.2 Only permitted, verified, and tested software from authorised sources shall be installed.

5.6.1.3 The system shall have port security implemented on network devices to prevent the use of unused ports.

5.6.1.4 There shall be no unmanaged network devices on the system

5.6.1.5 The system shall employ protection mechanisms to prevent, detect, report, and mitigate the effects of malicious code or unauthorised software.

5.6.1.6 The system shall provide the capability to update the protection mechanisms.

5.6.1.7 The system shall provide the capability to support verification of the intended operation of security functions and report when anomalies are discovered during FAT, SAT, and scheduled maintenance. These security functions shall include all those necessary to support the security requirements specified in this standard.

5.6.1.8 The system shall provide the capability to detect, record, report and protect against unauthorised changes to software and information at rest.

5.6.1.9 The system shall validate the syntax and content of any input which is used as an input that directly impacts the action of the system.

5.6.1.10 The system shall provide the capability to set outputs to a predetermined state if normal operation cannot be maintained because of an attack.

5.6.1.11 The system shall identify and handle error conditions in a manner such that effective remediation can occur. This shall be done in a manner which does not provide information that could be exploited by adversaries to attack the OT unless revealing this information is necessary for the timely troubleshooting of problems.

5.6.1.12 The system shall provide the capability to protect the integrity of sessions.

5.6.1.13 The system shall reject any usage of invalid session IDs.

5.6.1.14 The system shall protect audit information and audit tools (if present) from unauthorised access, modification, and deletion.

5.6.1.15 The system shall provide the capability to limit the number of concurrent sessions per interface for any given user (human, software process or device) to a configurable number of sessions.

5.6.1.16 The system shall provide the capability to employ malicious code protection mechanisms at all entry and exit points.

5.6.1.17 The system shall provide the capability to support partitioning of data, applications and services based on criticality to facilitate implementing a zoning model (Section 5.6.5 and supporting guidance refers).

5.6.1.18 The system shall provide the capability to operate in a degraded mode during a Denial of Service (DoS) event.

5.6.1.19 The system shall provide the capability to manage communication loads (such as using rate limiting) to mitigate the effects of information flooding types of DoS events.

5.6.1.20 The system shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion.

Note: For safety critical and service critical systems the following additional requirements shall apply:

5.6.1.21 Central management and reporting for malicious code protection.

5.6.1.22 Automated mechanisms for security functionality verification.

MAYOR OF LONDON
Transport for London
TfL RESTRICTED

5.6.1.23	Security functionality verification during normal operation.
5.6.1.24	Automated notification about integrity violations.
5.6.1.25	Hardware and software inventory.
5.6.1.26	Discovery tooling.

5.6.2 Configuration Management / Change Control

TfL must implement configuration management processes to control modifications to hardware, firmware, software, and documentation to ensure that the system is protected against improper modifications prior to, during, and after system implementation.

The project must meet the following minimum baseline requirements:

5.6.2.1 The current OT network configuration and device configurations must always be known and documented.

5.6.2.2 A formal change management process should be established to ensure that all modifications to an OT network meet, or exceed, the security requirements as defined in the system specifications or low-level design.

5.6.2.3 Risk assessment must be performed on all changes to the OT network that could affect security, including configuration changes, the addition of network components, and installation of software.

5.6.2.4 There should be restricted access to configuration settings of OT components.

5.6.3 System and Information Integrity

TfL must maintain system and information integrity to ensure that sensitive data has not been modified or deleted in an unauthorised and undetected manner.

The project must meet the following minimum baseline requirements:

5.6.3.1 There shall be controls implemented for malware detection, spam and spyware protection and intrusion detection.

5.6.3.2 An alert should be raised if these controls are triggered.

5.6.4 Malware Detection

TfL must ensure that malware detection products are deployed as widely as possible.

Malware detection products evaluate files on a computer's storage devices against an inventory of known malware signature files.

Anti-malware software can be deployed on workstations, servers, firewalls, and handheld devices, but may not be appropriate for operational devices.

Anti-malware tools only function effectively when installed, configured, running full-time, and maintained properly against the state of known attack methods and payloads.

The project must meet the following minimum baseline requirements:

5.6.4.1 Anti-malware products must be installed on all devices that can support it. This includes, but is not limited to, Windows, Unix, Linux systems, etc. used as consoles, engineering workstations, data historians, HMIs and general-purpose SCADA and backup servers.

5.6.4.2 Malware detection shall be implemented with anti-malware protection and / or whitelisting. Whitelisting must:

- Prevent the execution of all unauthorised software.
- Provide an alert when unauthorised software attempts to run.
- Report the list of authorised software and versions that are on the OT assets.

5.6.4.3 Updates for anti-malware products installed on the OT Network must only be obtained from secure sources (i.e. a dedicated anti-malware distribution server, located within a DMZ outside the OT network (Section 5.6.5 refers)).

5.6.4.4 Anti-malware tools shall be the subject of a dedicated compatibility testing routine to ensure their use does not impact system performance.

5.6.4.5 Malware protection shall be in place at all physical and logical network entry and exit points (e.g. Which may also need the use of 'Sheep Dips').

5.6.5 Network Segmentation

TfL must ensure that the networks and information systems supporting the TfL services are segregated into appropriate security Zones as defined in the Zone and Conduit model (See Section 4.6 of the supporting Guidance document).

Network segmentation and the level of protection it provides will vary greatly depending on the overall network architecture. Logically segmenting networks based on their functionality provides some measure of protection but may still lead to single-points-of-failure if a network device is compromised. Physically segmenting networks provides another level of protection by removing that single-point-of-failure case but will lead to a more complex and costly network design.

The project must meet the following minimum baseline requirements:

5.6.5.1 The system design shall group key OT devices into separate Zones with common security levels to manage security risks and to achieve a desired target security level for each Zone.

5.6.5.2 The system shall be separated into Zones and each Zone shall have a clearly defined security level.

5.6.5.3 There shall be enforced Conduits between Zones.

5.6.5.4 There shall be firewalls between Zones of differing security levels.

5.6.5.5 There shall be Access Control Lists (ACLs) between Zones of common security levels.

5.6.5.6 There shall be a DMZ between the IT and OT Networks.

5.6.5.7 There shall be no direct Internet access to or from the OT Network.

5.6.5.8 An OT DMZ shall be used for all outbound connectivity.

5.6.5.9 There shall be Virtual Local Area Networks (VLANs) to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.

5.6.5.10 The design shall ensure there are simple data flows between systems, devices, and interfaces to enable effective monitoring.

5.6.5.11 Any connections to external networks or other systems must occur through managed interfaces consisting of appropriate boundary protection devices (for example, proxies, gateways, routers, firewalls, unidirectional gateways, guards and encrypted tunnels) arranged in an effective architecture (for example, firewalls protecting application gateways residing in a DMZ). These connections must be necessary for operational and business purposes and subject to risk assessment.

5.6.5.12 High-risk or critical systems shall be subject to a risk assessment to determine if they should be isolated from or employ a barrier device to separate them from other Zones with different security levels or risks i.e. unidirectional gateways.

5.6.5.13 The system shall provide the capability to support partitioning of data, applications and services based on criticality to facilitate the zoning model. This may require that some servers may need to be duplicated on the control system network to support normal network features, for example Dynamic Host Configuration Protocol (DHCP), Domain Name Service (DNS) or local Certificate Authorities (CAs).

5.6.5.14 Systems shall only be connected to external networks where absolutely necessary and must undergo business justification and further risk assessment to provide justification.

Note: For safety critical and service critical systems the following additional requirements shall apply:

5.6.5.15 Independence from non-control system networks.

5.6.5.16 Greater logical and physical isolation of critical networks.

5.6.5.17 Island mode (physical isolation of critical networks).

5.6.5.18 Fail close operation.

5.6.5.19 Uni-directional gateways or data diodes.

5.6.6 Zone boundary protection

TfL must ensure that the system shall provide the capability to monitor and control communications at Zone or segmentation boundaries to enforce the compartmentalisation defined in the Zone and Conduits model.

The project must meet the following minimum baseline requirements:

5.6.6.1 The system shall provide the capability to monitor and control communications at Zone boundaries.

5.6.6.2 The system shall provide the capability to deny network traffic by default and allow network traffic by exception (also termed deny all, permit by exception).

5.6.6.3 In response to an incident, it may be necessary to break the connections between different network segments. In that event, the services necessary to support essential operations should be designed and maintained in such a way that the devices can continue to operate properly and/or shutdown in an orderly manner.

5.6.6.4 System boundary protections at any designated alternate location should provide the same levels of protection as that of the primary site.

5.6.7 General purpose person-to-person communication restrictions

TfL shall ensure that the system shall provide the capability to restrict or prevent general purpose person-to-person messages from being received from users or systems external to the system.

The project must meet the following minimum baseline requirements:

5.6.7.1 The system shall restrict email or other messaging solutions that provide internal computer-to-external computer communications using outbound messages.

These internal-to external communications may be limited to the purpose of sending system alerts or other computer-generated information messages to users or systems external to the system.

5.6.7.2 The system shall utilise preconfigured messages to transmit alert or status information.

5.6.7.3 The system shall not allow users to attach files or other information to these outbound-only messages at the time the messages are created by the system.

Note: For safety critical and service critical systems the following additional mitigations shall apply:

5.6.7.4 Prohibit all general-purpose person-to-person communication.

5.6.8 Security configuration settings

TfL shall ensure that the system has the capability to be configured according to recommended security configurations (See Section 5.6.9).

The project must meet the following minimum baseline requirements:

5.6.8.1 The system shall provide an interface to support the management of network and security configuration settings.

5.6.8.2 The system shall be able to support monitoring and control of changes to the configuration settings.

Note: For safety critical and service critical systems the following additional requirements shall apply:

5.6.8.4 Implementation of an automated check process where the current security settings are automatically collected by an agent and compared to approved settings, with changes being alerted.

5.6.9 Secure Configurations

TfL shall ensure that the system has been configured according to recommended network and security configurations, aka system hardening.

If the manufacturer's recommended configurations are different to any configurations required by this standard, the differences must be reviewed and the most restrictive configuration applied, unless this would impact the safe and reliable operation of the system.

The project must meet the following minimum baseline requirements:

5.6.9.1 There shall be documentation detailing all applications, utilities, system services, scripts, configuration files, databases, and all other software required and the appropriate configurations, including revisions and/or patch levels for each of the computer systems associated with the system.

5.6.9.2 There shall be a documented list of services required for any computer system running control system applications or required to interface the control system applications. The list must include:

- All ports and services required for normal operation as well as any other ports and services required for emergency operation.
- Justification as to why each service is necessary for operation.

5.6.9.3 All software components that are not required for the operation and maintenance of the control system must be removed prior to FAT. This must include, but is not limited to:

- Games
- Device drivers for network devices not in use
- Instant messaging services
- Servers or clients for unused Internet services
- Software compilers in all user workstations and servers except for development workstations and servers
- Software compilers for languages that are not used in the control system
- Unused networking and communications protocols
- Unused administrative utilities, diagnostics, network management, and system management functions
- Backups of files, databases, and programs used only during system development
- All unused data and configuration files
- Sample programs and scripts
- Unused document processing utilities (Microsoft Word, Excel, PowerPoint, Adobe Acrobat, OpenOffice, etc.).

5.6.9.4 Unnecessary credentials shall be removed (preferred option) or disabled.

5.6.9.5 Unnecessary communication ports and media drives shall be disabled by logical (software) or physical (disconnection) means or secured with an engineered barrier.

5.6.9.6 The system BIOS shall be password protected to prevent unauthorised configuration changes, unless this is not technically possible, which must be recorded in the system risk register.

5.6.9.7 There shall be documentation covering components that have been removed and/or disabled, and justification for components that remain enabled.

MAYOR OF LONDON
Transport for London
TfL RESTRICTED

5.6.10 Remote Access

TfL must ensure that the system shall provide the capability to monitor and control all methods of access to the control system via untrusted networks.

The project must meet the following minimum baseline requirements:

5.6.10.1 Remote access services shall use secure methods such as VPN and SSH.

5.6.10.2 Remote access services must route through an OT DMZ.

5.6.10.3 An OT DMZ shall be the preferred means of controlled remote access to OT systems.

5.6.10.4 The system shall provide the capability to deny access requests via untrusted networks unless approved by an assigned role.

5.6.10.5 Telnet sessions shall not be permitted.

5.6.10.6 Dial up and line modems shall not be permitted.

5.6.10.7 The system shall provide the capability to terminate a remote session either automatically after a configurable period of inactivity or manually by the user who initiated the session (Section 5.1.2 refers).

5.6.10.8 The system shall employ a multifactor authentication scheme with an appropriate level of strength to positively identify a remote interactive user.

5.6.11 Vulnerability Management

TfL must ensure that there is the capability to manage vulnerabilities in the network and information systems to prevent disruption of TfL services.

It would be expected that vulnerability management would be a pan-TfL service, since a vulnerability could affect a component which is used in multiple systems or services and therefore required a coordinated approach across TfL, but individual projects must ensure that systems are designed to comply with the principles of vulnerability management and can be kept secure through life.

The project must meet the following minimum baseline requirements:

5.6.11.1 The system must be free of known vulnerabilities on handover to operational service. Where a vulnerability cannot be resolved, suitable alternative controls must be implemented and the vulnerability, with mitigating controls and a long-term resolution plan, recorded in the project risk register.

5.6.11.2 The system shall not be handed over with obsolete technology in place.

5.6.11.3 There shall be a process to monitor and analyse publicly known vulnerabilities relevant to the system to understand the risk. This will require access to documents covering the system and network configuration, high level design and asset register.

5.6.11.4 There shall be a process to ensure that both publicly announced and privately notified vulnerabilities in the system are tracked. Tracked vulnerabilities must be clearly tagged with both the OT system affected and the TfL services which could be impacted if the vulnerability was exploited.

5.6.11.5 There shall be a process to ensure that vulnerabilities being tracked can be assessed, prioritised, and mitigated.

5.6.11.6 There shall be a process to implement a temporary mitigation solution for a vulnerability which is not exposed outside the system boundary/security Zone of the system.

5.6.11.7 There shall be a process to implement a temporary mitigation solution for obsolete and/or unsupported technology while pursuing migration to supported technology.

5.6.11.8 Any temporary mitigation, whether for a vulnerability or obsolete technology, must be risk assessed and recorded in the system risk register. The project should consider that the vulnerability or obsolete technology could have a wider impact across TfL than the immediate system in question.

5.6.11.9 The system shall be capable of supporting regular tests or assessments undertaken to check for previously unknown vulnerabilities within the constituent components.

Due to the sensitive nature of OT networks and systems, operators need to carefully consider their approach to the testing of live OT, as system operation, availability and safety could be affected. Assurance could be gained without this additional risk by testing against non-operational environments or by testing individual components in a laboratory environment.

5.6.11.10 Vulnerabilities shall be rated according to the Common Vulnerability Scoring System (CVSS)

5.6.12 Patch Management

TfL must ensure that there is the capability to deploy patches in the network and information systems to prevent disruption of TfL services.

Patches are additional pieces of code that have been developed to address specific problems or flaws in existing software. They can be part of a general service improvement plan from the manufacturer or can be in response to a specific vulnerability.

It would be expected that patch management would be a pan-TfL service, since a patch could affect a component which is used in multiple systems or services and therefore required a coordinated approach across TfL, but individual projects must ensure that systems are designed to comply with the principles of patch management and can be kept secure through life.

Applying patches to Operating System (OS) components creates another situation where significant care should be exercised in the OT environment.

The project must meet the following minimum baseline requirements:

5.6.12.1 Systems are to be handed over into operation with the latest approved and validated software version and patch revision applied.

5.6.12.2 There shall be a systematic and documented patch management process which must operate throughout the operating life of the system.

5.6.12.3 Patches must be thoroughly tested to determine they do not impact the safe operation of the system and do not introduce unexpected side effects. Regression testing is advised.

5.6.12.4 Patches must only be deployed from known secure sources. The preferred source shall be a patch management server within the DMZ which should act as a repository for patches from external sources for planned or scheduled deployment.

5.6.12.5 Any patches which cannot be applied must be captured with the system risk register.

5.6.13 Time Synchronisation

TfL must ensure that time is synchronised across all systems and services.

The project must meet the following minimum baseline requirements:

5.6.13.1 The system shall synchronise with a dedicated time source through a secure interface.

5.6.13.2 The dedicated time source shall be protected from unauthorised modification.

5.7 Secure Management:

TfL must ensure that network and information systems that support the delivery of TfL services can be managed, operated, and maintained securely.

5.7.1 Secure Management

Systems shall be managed, operated, and maintained in a secure manner.

The project must meet the following minimum baseline requirements:

5.7.1.1 Dedicated devices shall be used for the maintenance and security management of OT systems.

5.7.1.2 Devices which will be used to manage and maintain systems shall be verified as free from unauthorised software and malware before being connected to conduct management or maintenance activities.

5.7.1.3 Systems shall only be administered and maintained by authorised privileged users.

5.7.1.4 Secure management processes and supporting technical information shall be documented as part of the system development process and handed over with the system into operational service.

5.7.1.5 Documents which support the system shall be stored and secured according to the criticality of the system or the impact of the loss of that system on the delivery of TfL services.

6 Detecting cyber security events

The following controls and considerations will contribute to detecting cyber security incidents within TfL's OT and establish the minimum baseline of cyber security measures for all new projects and upgrades to existing systems.

Safety and service critical systems must also be risk assessed and are expected to require additional controls above the minimum baseline, for which suggestions are shown in the notes and guidance.

6.1 Security Monitoring

TfL must ensure that systems have effective cyber security defences and the capability to detect cyber security events which affect, or have the potential to affect, the delivery of TfL services.

6.1.1 Monitoring coverage

TfL must ensure that data sources have been identified to support the timely identification of security events in the system.

The project must have the capability to meet the following minimum baseline requirements:

6.1.1.1 Security monitoring data shall be collected from identified data sources (Section 6.1.3 refers) to detect and identify security events in the system.

6.1.1.2 The monitoring shall detect the presence of known indicators of compromise on the essential components of the system.

6.1.1.3 Monitoring shall be conducted of all privileged activity on the system for suspicious or undesirable activity.

6.1.1.4 There shall be monitoring in place on all network gateways and critical devices, where possible.

6.1.1.5 There shall be network taps installed at the network choke point boundary between the OT system and any external systems.

6.1.1.6 There shall be network taps installed at the network choke point boundary between the OT control system and its subordinate Zones.

6.1.1.7 There shall be monitoring in place to collect essential information against critical services or applications (such as key servers).

6.1.1.8 There shall be monitoring in place to detect the connection of unauthorised devices to the system.

6.1.1.9 There shall be documented reporting mechanisms such that any monitoring alert can allow for a timely response to events.

6.1.1.10 There shall be a centralised logging server.

6.1.1.11 System logs shall be capable of being read locally and forwarded to the centralised logging server.

6.1.2 Securing Logs

TfL must ensure that logging data be held securely and read access to it should be granted only to accounts with a business need.

The project must meet the following minimum baseline requirements:

6.1.2.1 Only authorised personnel can view logging information.

6.1.2.2 There shall be no ability to modify or delete logging data within the specified retention period, after which it can be deleted.

6.1.2.3 The system shall protect audit information and audit tools (if present) from unauthorised access, modification, and deletion.

6.1.2.4 The system shall provide the capability for authorised humans and/or tools to access audit logs on a read-only basis.

6.1.2.5 The system shall allocate sufficient audit record storage capacity according to commonly recognised recommendations for log management and system configuration.

6.1.2.6 The system shall provide auditing mechanisms to reduce the likelihood of such capacity being exceeded.

6.1.2.7 The system shall provide the capability to alert personnel and prevent the loss of essential services and functions in the event of an audit processing failure.

6.1.2.8 The system shall provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.

It should be noted that either overwriting the oldest audit records or halting audit log generation are possible responses to audit storage capacity being exceeded but imply the loss of potentially essential forensic information.

Note: For safety critical and service critical systems, the following additional requirements shall apply:

6.1.2.9 Audit records on write once media.

6.1.3 Generating Alerts and Audit Records

TfL must ensure that data relating to potential security alerts is captured in the monitoring data and that alerts are triggered.

The project must meet the following minimum baseline requirements:

6.1.3.1 The system shall generate audit records about events occurring in the system.

6.1.3.2 Audit records should be sufficient in detail to monitor the effectiveness and proper operation of the security mechanisms in place on the system.

6.1.3.3 The system shall provide the capability to generate audit records relevant to security for the following categories:

- Access control
- User activity
- Request errors
- Operating system (System, User and Security) events
- Control system events
- Use or attempts to use mobile devices
- Connection of unauthorised devices
- Backup and restore events
- Configuration changes
- Potential reconnaissance activity

- Audit log events
- Anti-malware events
- Boundary device logs
- FTP Logs
- Proxy Logs
- VPN Logs.

6.1.3.4 The system shall provide timestamps for use in audit record generation.

6.1.3.5 Individual audit records shall include:

- Timestamp
- Source (originating device, software process or human user account)
- Category
- Type
- Event ID
- Event result.

6.1.3.6 Alerts shall be resolved to individual assets.

6.1.3.7 Actions shall be attributed to a specific human user.

6.1.3.8 Alerts shall be generated on suspicious activity linked to known indicators of compromise.

6.1.3.9 Security logs shall be reviewed regularly and, if possible, alerts should be reviewed almost continuously, in real time.

6.1.3.10 Security alerts shall be prioritised, investigated and appropriate action taken.

Note: For safety critical and service critical systems, the following additional requirements shall apply:

6.1.3.11 Internal time synchronisation.

6.1.3.12 Protection of time source integrity.

6.1.3.13 Non-repudiation for all users.

6.1.4 Identifying Security Incidents

TfL must ensure that security alerts are contextualised with knowledge of the threat and the systems, to identify those security incidents that require some form of response.

The project must meet the following minimum baseline requirements:

6.1.4.1 Updates for all signature based protective technologies are received at least monthly.

6.1.4.2 The system shall have the capability for updates to be implemented at least monthly.

6.1.4.3 There shall be a recognised source of threat information to support the identification of security issues.

6.1.4.4 Security alerts shall be prioritised, investigated and appropriate action taken.

6.1.5 Monitoring Tools and Skills

TfL must ensure that monitoring staff skills, tools, and roles, including any that are outsourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they protect.

The project must meet the following minimum baseline requirements:

6.1.5.1 The system shall meet the requirements for monitoring coverage (Section 6) and incident response (Section 7) are defined, with appropriate tools and techniques identified.

> Consideration should be given to aligning these tools and techniques with other systems for a more consistent and coordinated approach.

6.1.5.2 There shall be personnel in place who are responsible for the analysis, investigation and reporting of monitoring alerts covering both security and system performance.

> This could involve additional personnel to create additional capacity or require existing personnel to be updated on the new system.

6.1.5.3 There shall be defined roles and skills/competence requirements to ensure that monitoring personnel, together with other personnel such as operators, system administrators and third parties, are able to cover all parts of the monitoring and investigation process.

6.1.5.4 There shall be documentation to inform monitoring personnel which TfL services are supported by the assets being monitored so that alerts or investigations can be prioritised appropriately.

6.1.5.5 There shall be documented processes, procedures, and workflows for monitoring personnel to follow for the analysis, investigation and reporting of alerts.

> The project may have to update existing process for the new system or create new processes to support the new system.

6.1.6 Incident Reporting

TfL must ensure that the reporting requirements for cyber security incidents are clearly articulated and understood to ensure that the right information is provided to the right people in a timely manner to allow incidents to be resolved effectively.

The project must develop reporting processes and ensure that the system can generate the information required, reporting at the first available opportunity, to meet the following minimum baseline reporting requirements:

6.1.6.1 The theft or unexplained loss of cyber systems or assets, asset data which an attacker could use to improve the chances of a successful attack or circumvent installed security measures.

6.1.6.2 The unauthorised physical or electronic access to cyber systems.

6.1.6.3 The compromise of a Cyber Assurance of Physical Security Systems (CAPSS) verified system protecting a Railway Asset.

6.1.6.4 The occurrence of successful or suspected attempted jamming of radio communication systems such as (but not limited to) mobile phones, portable credit/debit card payment systems, radios, Global Positioning System (GPS) radio navigation systems or Global System for Mobile Communications-Railway (GSM-R).

6.1.6.5 The unauthorised addition or modification of software or data on cyber systems.

6.1.6.6 The unauthorised destruction or disruption of software or data.

6.1.6.7 The malware infection of assets or attempted cyber intrusion.

6.1.6.8 The unauthorised physical access to secure rooms.

6.1.6.9 All incident reports must be made to the TfL Security Operations Centre (SOC) at the earliest opportunity.

6.1.6.10 All incident reports relating to NIS systems must be made within 72 hours to the competent authority.

7 Minimising the impact of cyber security incidents

The following controls will contribute to minimising the impact of a cyber security incident on TfL's OT and establish the minimum baseline of cyber security measures for all new projects and upgrades to existing systems.

Safety and service critical systems must also be risk assessed and are expected to require additional controls above the minimum baseline, for which suggestions are shown in the notes.

7.1 Incident response and recovery planning

TfL must be prepared to restore TfL services following disruption as a result of a cyber incident and must ensure that there are well-defined and tested incident management processes in place, that aim to ensure continuity of essential functions in the event of system or service failure.

Mitigation activities designed to contain or limit the impact of compromise are also in place.

An incident response plan is the documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of incidents against an organisation's information systems. Response should be measured first and foremost against the "service being provided," not just the system that was compromised.

7.1.1 Business Continuity Plan

TfL must ensure that new systems and upgrades are included in the Business Continuity Plan, which will identify procedures for maintaining and/or re-establishing essential business operations while recovering from a significant disruption.

The project must meet the following minimum baseline requirements:

7.1.1.1 Recovery objectives shall be determined for the systems involved, based on business needs.

MAYOR OF LONDON
Transport for London
TfL RESTRICTED

7.1.1.2 An assessment shall be conducted to determine the impact to TfL services because of significant disruption or system loss.

7.1.1.3 Continuity plans shall be developed and implemented to ensure that business processes can be restored in accordance with recovery objectives.

7.1.1.4 The business continuity plan shall be updated with any specific roles and responsibilities for the new system.

7.1.1.5 There shall be backup and restore procedures that support the business continuity plan.

7.1.2 Response and Recovery Plan

TfL must ensure that cyber incident response plans are updated with new and updated systems.

The project must meet the following minimum baseline requirements:

7.1.2.1 The overall cyber incident response plan that identifies responsible personnel and defines actions to be performed by designated individuals shall be updated.

7.1.2.2 The various types of OT incidents should be identified and classified as to potential impact so that a proper response can be formulated for each potential incident.

7.1.2.3 The systems and supporting technologies required to restore operations are known, documented and in line with TfL business continuity, disaster recovery and risk management processes.

7.1.2.4 The incident response plan shall be communicated to all appropriate organisations.

7.1.2.5 The response plan shall be tested during system development, at least during FAT and SAT and shall be capable of being repeated at regular intervals once handed over to operations.

7.1.2.6 Develop procedures to support the activities as determined by the cyber elements of an incident response plan or dedicated cyber incident response plan. The procedures must document the actions to be taken in the event of a cyber security incident and those listed in Section 6.1.6.

7.1.2.7 Create offline and hardcopies of incident response plans and procedures.

7.1.3 System recovery

TfL must ensure that the system provides the capability to recover and reconstitute to a known secure state after a disruption or failure.

System recovery and reconstitution to a known secure state means that all system parameters (either default or configurable) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are re-established, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded and the system is fully tested and functional.

The project must meet the following minimum baseline requirements:

7.1.3.1 The sequence in which systems, networks and supporting technologies are recovered to restore the systems supporting the delivery of TfL services shall be known, documented, and shared when the system is handed over to operations.

7.1.3.2 The interdependencies between the systems and the supporting technologies shall be understood, documented, and shared when the system is handed over to operations.

7.1.3.3 The system shall provide the capability to switch to and from an emergency power supply without affecting the existing security state or enter a documented degraded mode.

7.1.3.4 There may be instances where compensating countermeasures such as physical door access control may be affected by loss of base power supply, in which case the emergency power supply should cover those associated systems. If this is not possible, other compensating countermeasures may be needed during such an emergency situation.

7.2 Backups:

TfL must ensure that there are accessible and secured current backups of data and information needed to recover network and information systems which support the TfL services.

7.2.1 Backups

TfL must ensure that there are backups of all systems, software, licenses, configurations, data, and other relevant information required to enable recovery of individual devices or entire networks and systems supporting the delivery of TfL services.

The project must meet the following minimum baseline requirements for backups from Section 5.5.7.

7.3 Incident lessons learned

TfL must ensure that following an incident or exercise, a root cause analysis shall be conducted to identify measures to prevent reoccurrence based upon incident or exercise.

7.3.1 Lessons Learned

TfL must ensure that lessons are learned from any incident or exercise and that documentation and processes are updated to reflect those lessons.

The project must meet the following minimum baseline requirements:

7.3.1.1 The details of an identified incident shall be documented to record the incident, the response and the lessons learned to update system documentation and response processes considering the incident or exercise.

7.3.1.2 Exercise scenarios should be developed and tested to ensure that different aspects of the response plan can be tested on a periodic, at least annual, basis. Lessons learnt from exercise tests shall be remediated prior to handover into operation.

8 Supporting Information

8.1 Background

Cyber security should be considered as an integral part of any review for any OT and where possible should be integrated into existing safety, environmental, operational or risk considerations. This should reflect that cyber could be a potential cause of a failure and needs to be captured as part of the response or recovery process, rather than a separate consideration.

8.2 Customer Considerations

Whilst cyber security for OT should not be at the forefront of customer considerations, it should form part of the wider safe, secure and reliable message.

9 Guidance

For further advice and guidance in support of this Standard contact the Cyber Security team CyberSecurityGRC@tfl.gov.uk

10 Person accountable for this document

Name	Job title
Paul Richardson	Cyber Security Assurance Manager

11 Definitions

Term	Definition	Source
Operational Technology	A collection of personnel, processes, hardware and software that can affect or influence the safe, secure and reliable operation of a physical process or asset.	Jargon Buster
Conduit	Security groupings for the communications of information into, out of and within the security Zones/networks	Jargon Buster
Internet	This public data network is considered hostile in the context of the ICS.	Jargon Buster
Protection Systems	Protection systems, Safety-Instrumented System and Emergency Shutdown Systems	Jargon Buster
Segregation	Physically or logically separating different Zones	Jargon Buster

Term	Definition	Source
Zone	A grouping of electronic assets that share common cyber security requirements	Jargon Buster

12 Abbreviations

Abbreviation	Meaning
CCTV	Closed Circuit Television
CPNI	Centre for the Protection of National Infrastructure
DMZ	De-Militarised Zone
FAT	Factory Acceptance Testing
HMI	Human Machine Interface
HR	Human Resources
ICS	Industrial Control System
IT	Information Technology
LAN	Local Area Network
OS	Operating System
OT	Operational Technology
PLC	Programmable Logic Controllers
RTU	Remote Terminal Units
SAT	Site Acceptance Testing
SCADA	Supervisory Control and Data Acquisition
SIS	Safety-Instrumented System
SMS	Short Message Service
SOC	Security Operations Centre
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

13 References

Document no.	Title or URL
R1770	Operational Technology Cyber Security - Framework
S1147	Surveillance and Security Systems
S1747	Physical Security of IT Equipment
S1770	Operational Technology Cyber Security - Governance
S1772	Operational Technology Cyber Security – Operations and Maintenance
S1782	Information Security Classification
G1771	Operational Technology Cyber Security – Projects and Upgrades Guidance
G1134	Personnel Security – Insider Threats
N/A	NIS CAF
HSE OG86v2	Cyber Security for Industrial Automation and Control Systems (IACS) Edition 2
IEC 62443-2-1	Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security

Document no.	Title or URL
	program
IEC 62443-3-3	Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels
N/A	CPNI Good Practice Guide – Process Control and SCADA Security
NIST SP800-82	Guide to Industrial Control System (ICS) Security
EN50128	Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems
EN50129	Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling
EN50519	Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems

14 Document history

Issue no.	Date	Changes	Author
A1	December 2021	New guidance document published in accordance with Change Request CR-15043.	Tim Parker

Transport for London

Invitation to Quote

Electric Vehicle Infrastructure Delivery (EVID)
Tranche 2, Batch 1

Volume 2

Appendix K_2

Cyber Security Operations and Maintenance

COMMERCIAL IN CONFIDENCE

TfL Restricted

Standard

S1772 A1 Operational Technology Cyber Security - Operations and Maintenance

Contents

1 Purpose 3

2 Scope 3

2.1 Operational Technology (OT) definition 3
2.2 Examples 4

3 Requirements 5

3.1 Protecting against cyber attack 6
3.2 Detecting Cyber Security events 7
3.3 Minimising the impact of Cyber Security incidents 7

4 OT Lifecycle 7

4.1 Good Practice Principles 8
4.2 OT Project Lifecycle Requirements 9
4.3 The Purdue model and Secure OT Design 12

5 Protecting against cyber attack 12

5.1 Identity and access control 12
5.2 Data Security 19
5.3 Personnel Security 21
5.4 Physical Security 24
5.5 Network Security 26
5.6 System Security 30
5.7 Providing Secure Management 40

6 Detecting Cyber Security events 41

6.1 Security Monitoring 41

7 Minimising the impact of Cyber Security incidents 46

7.1 Incident response and recovery planning 47
7.2 Backups 48
7.3 Incident lessons learned 49

8 Supporting Information 49

8.1 Background 49
8.2 Customer Considerations 49

9 Guidance 49
10 Person accountable for this document 50
11 Definitions 50
12 Abbreviations 50
13 References 51
14 Document history 52

1 Purpose

This standard describes the Cyber Security requirements for operating and maintaining in a secure manner all Operational Technology (OT) which is used to support services within Transport for London (TfL).

2 Scope

This standard applies to TfL staff and partners with responsibility for operating and maintaining OT. It applies at all times when operating or maintaining OT.

2.1 Operational Technology (OT) definition

Operational Technology is a collection of personnel, processes, hardware, and software that can affect or influence the safe, secure, and reliable operation of a physical process or asset.

These include, but are not limited to:

- Signalling for rail, road and marine transport, train management, Supervisory Control and Data Acquisition (SCADA), building management and access control, Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), intelligent electronic devices, networked electronic sensing and control, and monitoring and diagnostic systems.

In this context, process control systems include basic process control system and Safety-Instrumented System (SIS) functions, whether they are physically separate or integrated.

- Associated information systems such as advanced control, dedicated equipment monitors, graphical interfaces, process historians, and plant information management systems.
- Associated internal, human, network, or machine interfaces used to provide monitoring, control, and safety operations functionality.

As an owner and operator of physical transport assets, TfL has an extensive estate of OT systems and devices across a wide range of its underground and surface operations.

There are OT systems which are clearly OT such as traction power, tunnel ventilation, fire detection, and systems which are clearly Information Technology (IT) such as Human Resources (HR) and email. However, there are systems where the distinction is not as clear, such as CCTV and ticket barriers.

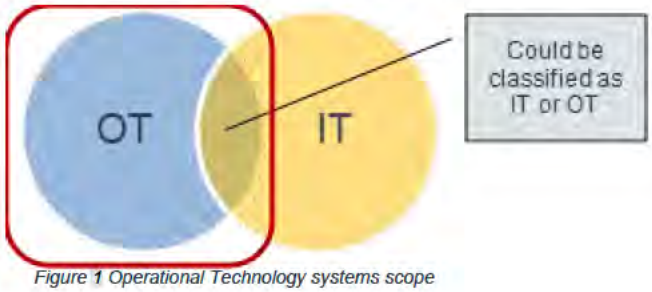


Figure 1 Operational Technology systems scope

MAYOR OF LONDON
Transport for London
TfL RESTRICTED

2.2 Examples

In this section we provide some examples of systems which may or may not be considered or recognised as OT.

2.2.1 Example OT systems

Examples of OT systems installed in London Underground and Surface Transport that are clearly OT include, but is not limited to:

- Power management systems (traction and general power)
- Energy monitoring
- Signalling systems
- Road traffic signals
- Rolling stock
- Communication networks used by OT (e.g. Surface WAN/Connect/Station LAN)
- Control and information systems
- Track systems
- Station systems (e.g. escalator and elevator control)
- Fire detection and suppression systems
- Civil Systems / Tunnel Systems
- Building management systems and building automation systems
- Heating, ventilation and air conditioning (HVAC) systems
- Security and access control systems (e.g. swipe card or key fob)

2.2.2 Example of systems which can be OT or IT

Some systems may be defined as OT or IT, which is usually dependent on the context. To determine if the system is OT or IT, refer to the definition in section 2.1 above and apply the test of whether the systems "can affect or influence the safe, secure, and reliable operation of a physical process or asset." If the answer to this is "Yes", then the system is OT, otherwise it is IT. It the answer is not clear, then refer to the supporting bullet points in the definition to for tests, such as whether the system provides "sensing" or "control", for example.

Some common edge cases which may be classified as OT or IT are given below:

CCTV and One Person Operation (OPO) CCTV – If the CCTV system (cameras and recorders) are networked then they would come under the definition as "networked electronic sensing" and "monitoring" in the definition above. CCTV which is monitoring an area (e.g. an underground station platform) controlled by other OT (e.g. BMS or signalling) should be classified as OT. CCTV which is not used directly to deliver or support delivering a service (e.g. Head Office CCTV for security monitoring) should be classified as IT.

MAYOR OF LONDON
Transport for London
TfL RESTRICTED

Lighting controls – Simple manual lighting controls are unlikely to be OT. Automated, remotely controlled or monitored lighting control systems for stations, road and rail tunnels, ferry terminals, are likely to be OT as they can affect the reliable operation of the lighting and of services.

HVAC – Reasonably modern HVAC systems in stations, tunnels and buildings (e.g. Victoria coach station) will have a control system which may be linked into a BMS. They may also have remote access from a facilities management and/or maintenance company.

Ticket barriers – A particular physical access control system which not only has card readers and controllers (OT) but will also link to ticketing systems which will be in the IT network.

Timetabling – Scheduling bus and train services with the timetabling system (IT) may need to interface to other OT systems, such as train management systems. The timetabling system could be considered as OT because it can "affect or influence the safe, secure, and reliable operation" of services.

2.2.3 Alignment to Purdue Model

A complimentary approach to determining if a system should be defined as OT or IT is to refer to the Purdue Model, G1772 Section 4 refers, where OT systems and services sit in Levels 0 to 3 in the Model and IT systems and services sit in Levels 4 and 5 of the Model.

3 Requirements

This standard states the mandatory requirements for OT Cyber Security during operations and maintenance and is aligned to the Network and Information Systems (NIS) Regulations (2018) and the International Electrotechnical Commission IEC 62443 series of standards for OT Cyber Security, in particular IEC 62443-3-3 system security requirements and security levels. It forms part of a wider framework of standards and guidance (R1770) for Operational Technology Cyber Security in TfL. The standard should be read in tandem with the associated guidance (G1772).

Each system will have been subject to a risk assessment during development to determine the cyber risk and to identify any additional controls required above that of the established minimum-security baseline or concessions which might be necessary where the minimum baseline cannot be met. This risk assessment and associated risk register will form part of the handover document set before the system is taken into live service, however the risk assessment will have to be revisited regularly throughout the operational life of the system.

Notwithstanding this, the minimum Cyber Security baseline established within this standard is the set of minimum Cyber Security requirements for ALL new or upgraded OT which support TfL services. It should also be considered as best practise for protecting legacy or established services during operations and maintenance activities, whilst recognising that these systems may not have been designed to incorporate Cyber Security controls and therefore alternative mitigation measures may have to be adopted.

MAYOR OF LONDON
Transport for London
TfL RESTRICTED

The baseline is intended to prevent the unauthorised disclosure of information to an entity actively searching for it using simple means with low resources, generic skills, and low motivation. These requirements are applicable to all OT assets including, but not limited to, Intelligent End Devices, Remote Terminal Units, Microcontrollers, Programmable Logic Controllers, Sensors, Actuators, Servers, Workstations, and Network Devices.

Concessions or non-compliance to the requirements established within this standard must have appropriate mitigating controls implemented and follow the formal engineering concession process. Any risks arising from the concession must have been registered in the project risk register, which is then transferred to the system owner and maintained as the system risk register.

The standard is intended to direct staff and partners working for TfL to understand and adopt the necessary steps to protect against cyber threats, detect a cyber incident and respond to a cyber incident when operating and maintaining OT which supports the delivery of TfL services safely and reliably.

Not all elements of the standard are solely the responsibility of the staff and partners responsible for the respective OT system; in some areas, TfL will have to have organisational processes or shared services, such as monitoring, in place to support these requirements and the OT systems will have to have the capabilities to apply the requirements.

For example, if an individual moves role, there needs to be recognition at an organisational level that their access privileges must be reviewed, but the system must have appropriate mechanisms to ensure access controls can be enforced and updated.

It is important to note that this standard closely mirrors Operational Technology Cyber Security – Projects and Upgrades (S1771) and the two documents have been written in parallel, since the Cyber Security requirements are carried forward from design into operation.

The key difference is that for Operations and Maintenance the emphasis is on **operating** and **supporting** the OT securely and according to established process to limit the likelihood and impact of a cyber incident, so the broader guidance remains to give context and build understanding of why the security controls are important. For Projects and Upgrades, the emphasis is more focused on **designing** and **implementing** the OT in a secure way, such that the cyber risk is mitigated as far as practicable and that the controls are appropriate to the risk.

Cyber Security considerations or controls are grouped according to the following security principles and the components are explained in the following sections.

3.1 Protecting against cyber attack

The requirement is that TfL will have proportionate security measures in place to protect TfL services and systems from cyber-attack.

The underlying principle is that TfL defines, implements, communicates, and enforces appropriate policies, standards, processes and procedures that direct its overall approach to securing systems and data that support delivery of TfL services.

3.2 Detecting Cyber Security events

The requirement is that TfL will have the capabilities to ensure security defences remain effective and to detect Cyber Security events affecting, or with the potential to affect, TfL services.

The underlying principle is that TfL monitors the security status of the networks and systems supporting the delivery of TfL services to detect potential security problems and to track the ongoing effectiveness of protective security measures.

3.3 Minimising the impact of Cyber Security incidents

The requirement is that TfL will have the capabilities to minimise the impact of a Cyber Security incident on TfL services, including the restoration of those services where necessary.

The underlying principle is that TfL has well-defined and tested Cyber Security incident management processes in place, that aim to ensure continuity of essential services in the event of an incident affective systems or services.

4 OT Lifecycle

All OT projects and operational systems must undertake Cyber Security activities and implement Cyber Security controls throughout both the project lifecycle as well as the operational lifecycle. For the purposes of this standard, the focus is on operating and maintaining OT systems securely during the operations phase, but the overall lifecycle is shown in Figure 1 to highlight that the operations phase is part of a much wider development process.

As such, lifecycle phases for which projects are responsible are summarised in this standard and only the Operations phase retained in full. For a full description of the OT Lifecycle, refer to S1771 Operational Technology Cyber Security – Projects and Upgrades, Section 4.

For staff and partners who are responsible for operating OT systems, they should understand that the project will deliver an OT system which is secure by design and capable of being operated in a “cyber-secure” manner and there will be end-of-life activities necessary to dispose of the system securely.

Figure 1 below details the OT Lifecycle.

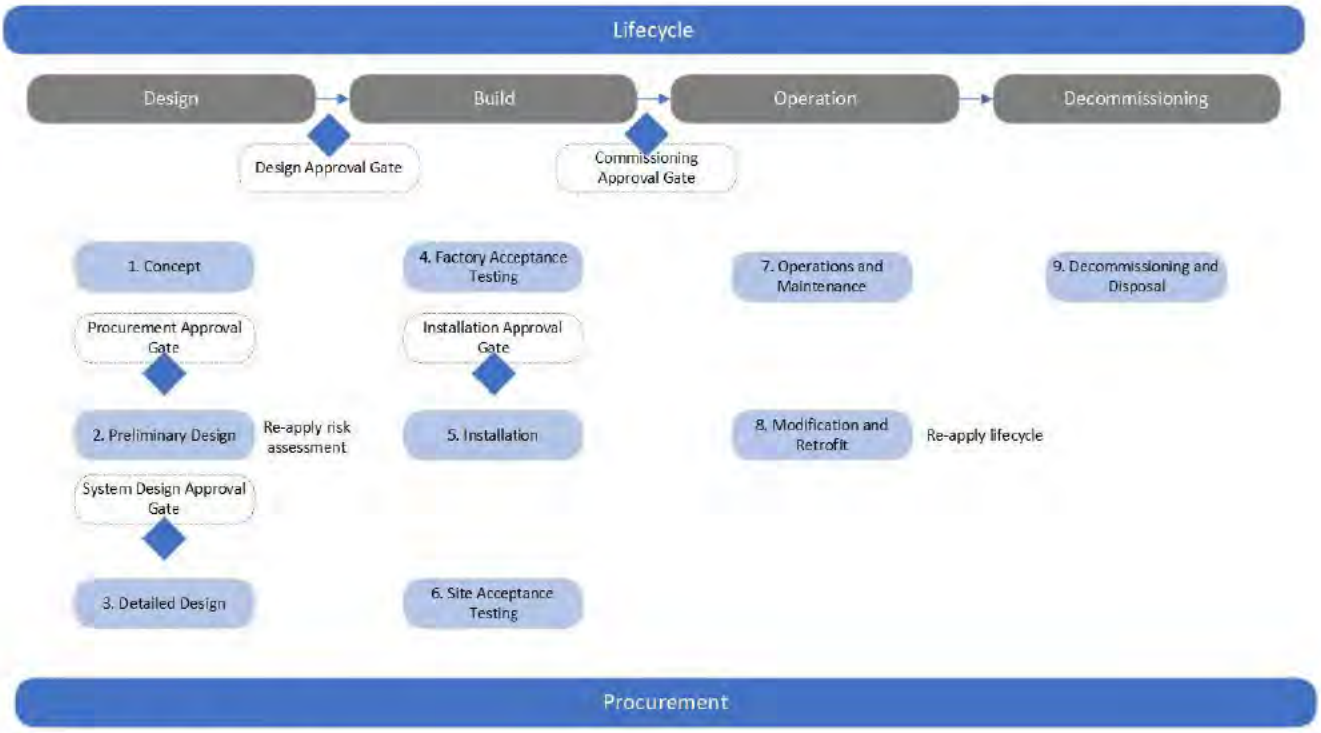


Figure 1 - OT Lifecycle

Implementing security protection measures into OT can be more difficult and costly once systems have been built and deployed. Even more important is that bolting on security measures to either in-service OT, or late in the development cycle of that OT, is often less effective than building them in at the beginning. Dealing with security risks by integrating protection measures into the OT early in its lifecycle is more effective, avoids overruns, is usually less costly and can often be a business enabler.

4.1 Good Practice Principles

To effectively manage the OT lifecycle within the organisation there are five good practice principles which bridge the gap between the lifecycle and Cyber Security frameworks and bring manageable actions to supporting the lifecycle.

The good practice principles are to:

- Ensure regulatory and security requirements are included in procurement and penalties are flowed down
- Ensure OT systems are secure by design
- Manage security through OT system construction
- Manage operational security
- Managing security risks during decommissioning and disposal.

MAYOR OF LONDON
Transport for London
TfL RESTRICTED

Further detail for each principle is contained in the supporting guidance document, G1772 Operational Technology Cyber Security – Operations and Maintenance.

4.2 OT Project Lifecycle Requirements

The following activities take place during the OT project lifecycle:

4.2.1 Concept Phase

4.2.1.1 The early development of a system concept, which will include initial risk assessments and cyber threat modelling.

4.2.2 Preliminary Design Phase

4.2.2.1 Developing the concept through early design activities to include the production of:

- High Level or Concept Design
- Draft Network specifications and proposed configurations
- Draft interface specifications
- Draft Cyber Security plan
- High Level Security Architecture.

4.2.3 Detailed Design Phase

4.2.3.1 Refining the preliminary design to a final design, including:

- Low Level or Detailed Design
- Network specifications and configurations
- Network traffic profile and expected communication paths
- Interface specifications
- Cyber Security plan
- Security Architecture, including Zone and Conduit model.

4.2.3.2 The design process will include consideration of incident management arrangements, secure development processes and testing arrangements.

4.2.4 Factory Acceptance Testing Phase

4.2.4.1 Functional testing of the system, including Cyber Security controls within the constraints of a factory setting. Staff and partners who are responsible for operating the system would expect to be involved in the Factory Acceptance Testing (FAT) phase so they can start to understand the system.

4.2.5 Installation Phase

4.2.5.1 The system is installed in the operational location. During this phase, staff and partners will receive Cyber Security training relating to the Cyber Security requirements, controls, and deliverables of the system.

4.2.6 Site Acceptance Testing Phase

4.2.6.1 Functional testing of the system, including Cyber Security controls within the constraints of a non-operational site setting.

4.2.6.2 Successful site acceptance testing will form the key determination of operational readiness.

4.2.7 Operations and Maintenance Phase

Documentation

4.2.7.1 The project shall provide staff and partners who are responsible for the OT system with documentation covering the design of the Cyber Security controls and their ongoing operation and maintenance.

4.2.7.2 As a minimum, the following documentation is to be provided for handover:

- Operational manuals
- Network specifications and configurations
- Baseline network traffic plan
- Cyber Security plans
- Asset Register
- High Level or Concept Design Document
- Low Level or Detailed Design Document.

Handover into Operation

4.2.7.3 The staff and partners who are responsible for the OT system must receive documentation to confirm that all the Cyber Security controls have been verified and validated as functional at handover.

4.2.7.4 The staff and partners who are responsible for the OT system must receive documentation to confirm that, where possible, identified risks and remediations have been closed out and that appropriate mitigating controls have been implemented where this has not been possible.

Training

4.2.7.5 The System Owner and Lead Maintainer must receive a comprehensive training program encompassing the entire Cyber Security program, developed security plans as well as the technical features and implementation details of the solutions developed/deployed during the project lifecycle.

Operational Lifecycle

4.2.7.6 The System Owner shall maintain an up-to-date asset register of all hardware and software components.

4.2.7.7 The System Owner shall implement and maintain the necessary processes and procedures to meet the requirements within this Standard.

4.2.7.8 The System Owner shall undertake periodic reviews of security controls, processes and procedures as identified within this Standard.

4.2.7.9 The System Owner shall undertake continuous verification and validation of Cyber

MAYOR OF LONDON
Transport for London
TfL RESTRICTED

Security controls and activities

4.2.7.10 The System Owner shall review Cyber Security risks on a periodic basis and no less than every 12 months

4.2.8 Modifications and Retrofit Phase

Operation and Maintenance

4.2.8.1 Prior to any modification of an OT asset, a Cyber Security risk assessment must be conducted to confirm that any temporarily disabled security features will not significantly impact the overall security posture of the OT asset during modification.

4.2.8.2 For any OT asset modification, the overall security posture of the of the current Cyber Security plan should be considered to ensure that the maintenance of the program provides assurance that implemented controls remain in place, and continue to operate correctly, and that the program itself continues to remain effective.

Secure Supply Chain

4.2.8.3 The staff and partners who are responsible for the OT system must ensure that secure supply chain requirements apply to both hardware and software assets.

4.2.8.4 There must be an ongoing process to protect the supply chain for OT assets. This process must contain adequate plans, processes, procedures, and registers to continually demonstrate to the system owner that the supply chain remains secure.

4.2.8.5 The secure supply chain must be used throughout the project or system lifecycle.

4.2.8.6 There must be controls in place to protect the systems during their physical or logical transport ensuring that the assets are not vulnerable to subversion, including malicious code insertion, counterfeit insertion, and tampering.

4.2.8.7 The secure supply chain process must be extended to third party products which are incorporated into the system.

4.2.8.8 The secure supply chain process must address and continually demonstrate the following during the project or contract lifecycle:

- Chain of custody practises and updated documentation.
- Inventory management including the location and protection of physical and logical assets including spare parts.
- Information protection
- Secure digital products delivery
- Trusted channels and controls to ship assets including tamper-proof packaging
- Controls to detect unauthorised access and/or alteration throughout the delivery process
- Cascading of these Cyber Security requirements to the entire supply chain
- Collection and preservation of evidence demonstrating security of the supply chain.

4.2.9 Decommissioning and Disposal Phase

4.2.9.1 There must be procedures in place to address decommissioning and disposal of OT assets (including media) in a controlled and secure manner, to avoid disruption to interfacing OT assets and disclosure of sensitive information.

4.3 The Purdue model and Secure OT Design

Sections 4.4 to 4.8 of the guidance document (G1772) provide knowledge and understanding which support the good practice principles in Section 4.2 and the OT Project lifecycle requirements in Section 4.3.

5 Protecting against cyber attack

The following controls will contribute to protecting TfL's OT against cyber-attack and establish the minimum baseline of Cyber Security measures for operating and maintaining new or upgraded systems securely. The minimum baseline Cyber Security measures should be adopted when operating or maintaining any OT supporting TfL services, recognising that legacy systems may not have been designed with these Cyber Security controls in place. Hence a risk assessment to be carried out and if required, the concession processes to be followed and work to close out any gaps.

Safety critical and service critical systems will have been risk assessed at the design stage and are expected to require additional controls above the minimum baseline, for which suggestions are shown in the notes.

5.1 Identity and access control

TfL must assure good management and maintenance of identity and access control for the networks and information systems supporting TfL services.

The requirement is that the system owner will have to maintain a list of all users (humans, software processes and devices) and to determine for each control system component the required level of Identity and Access Control (IAC) protection.

Access control is the method of controlling who or what entities can access premises and systems, as well as the type and level of access that is permitted. There are three key aspects associated with access control:

- account administration
- authentication
- authorisation.

All three aspects shall work together to establish a sound and secure access control strategy. Account administration is the method associated with granting and revoking access accounts and maintaining the permissions and privileges provided under these accounts to access specific resources and functions on the physical premises, network, or system. Access accounts should be function or role-based and may be defined for individuals, groups of individuals functioning as a crew or for devices providing a function.

The detailed requirements are aligned to the headings below to group requirements under common functions and to support traceability to the NIS regulations where required.

5.1.1 Account administration

As an organisation, TfL must ensure, on an ongoing basis, that only appropriate individuals or entities have accounts that allow access and that these accounts provide appropriate access privileges.

The system owner must ensure compliance with the following minimum baseline requirements:

5.1.1.1 Access shall be granted, changed, or terminated on the authority of an appropriate manager or system owner.

5.1.1.2 A record shall be maintained of all access accounts, including details of the individual(s) and devices authorised to use the account, their permissions, and the authorising manager.

5.1.1.3 Access accounts shall be suspended or removed as soon as they are no longer needed, for example in the event of a job change. 3rd parties engaged on the support and maintenance of systems are required to notify TfL of Joiners, Movers and Leavers.

5.1.1.4 All established access accounts shall be reviewed three-monthly to ensure that the accounts only provide the minimum required permissions.

5.1.1.5 The use of default accounts and passwords is forbidden.

5.1.1.6 There shall be no default or test credentials present/enabled on the system during operation. Passwords for access accounts shall be changed from default or test credentials before the system is handed into operation.

5.1.1.7 Periodic reviews of compliance, minimum six-monthly, to the account administration process should be performed.

5.1.1.8 Implement and maintain procedures for the creation, distribution, management and administration of user accounts.

Note: For safety critical and service critical systems the following additional requirements shall apply:

5.1.1.9 Unified account management (for example, an Active Directory service supporting multiple systems within a security Zone)

5.1.2 Authentication

As an organisation, TfL must positively identify network users, hosts, applications, services, and resources for computerised transaction so that they can be given the rights and responsibilities associated with the accounts they have been granted under account administration.

The system owner must ensure compliance with the following minimum baseline requirements:

5.1.2.1 All users must be authenticated before using an application or system.

5.1.2.2 Anonymous authentication shall not be permitted.

5.1.2.3 There shall be no hard-coded credentials in the system.

5.1.2.4 Root or administrator level accounts shall not be used as main credentials.

5.1.2.5 All default credentials must have been changed by FAT.

5.1.2.6 All system administrator access accounts and application configuration access accounts shall have strong authentication practices (such as requiring strong passwords or Multi Factor Authentication (MFA).

5.1.2.7 There shall be no use of SMS for MFA (alternatives are one-time passcodes from an app like Google Authenticator or hardware MFA).

Where this is not technologically achievable, possible compensating controls could include separate physical or electronic entrance control technologies or administrative practices, such as a two-person rule. In large scale or distributed systems, the use of a centralised access control system, such as LDAP or Radius, should be considered.

5.1.2.8 After 3 failed login attempts by a local or remote user, the system will disable the associated access account for 3 hours. There may need to be exceptions for local accounts on systems where constant access is required, such as Human Machine Interfaces (HMIs) in control rooms. Such exceptions must be covered by the concessions process and be recorded in the system risk register.

5.1.2.9 After 30 minutes of inactivity, a local or remote user will be required to re-authenticate before the user can re-access the system. There may need to be exceptions for local accounts on systems where constant access is required, such as HMIs in control rooms. Such exceptions must be covered by the concessions process and be recorded in the system risk register.

5.1.2.10 The system shall not allow multiple concurrent logins.

5.1.2.11 The system shall not allow applications to retain authentication data between sessions.

5.1.2.12 All access attempts to critical systems should be recorded and retained in a log file for a minimum period of three months.

5.1.2.13 Log Files should be reviewed weekly for successful and failed access attempts as well as unusual or unexpected activity such as out of hours access or attempts to access the system by unauthorised users.

5.1.2.14 Systems should employ an authentication scheme (such as X.509) for task-to-task communication between applications and devices.

Note:	For safety critical and service critical systems the following additional requirements shall apply:
5.1.2.15	MFA for untrusted networks.
5.1.2.16	MFA for all networks.

MAYOR OF LONDON
Transport for London
TfL RESTRICTED

5.1.3 Authorisation

As an organisation, TfL must grant access privileges to resources after successful authentication of the user and identification of their associated access account. The privileges granted are determined by the account configuration set up during the account administration step in the business process.

The system owner must ensure compliance with the following minimum baseline requirements:

5.1.3.1 There must be clearly documented rules that define the privileges authorised for access accounts which are aligned to the job roles for the system. These rules must follow the principles of least privilege.

5.1.3.2 The system must apply these rules to all users upon authentication.

5.1.3.3 Access accounts must be role based to manage access to appropriate information or systems for that user's role.

5.1.3.4 Safety implications shall be considered when defining roles.

Note: For safety critical and service critical systems the following additional requirements shall apply:

5.1.3.5 Unique identification and authorisation.

5.1.3.6 Hardware security for software process identity credentials.

5.1.4 Passwords

As an organisation, TfL must ensure that for control systems utilising password-based authentication, the control system shall provide the capability to enforce configurable password strength based on minimum length and variety of character types.

The system owner must ensure compliance with the following minimum baseline requirements:

If an OT system does not have the capabilities to meet all the password requirements, a concession must be raised.

5.1.4.1 Maintain the systems capability of a configurable password management facility to allow passwords to be selected according to the requirements in 5.1.4.2.

5.1.4.2 Passwords must meet the following requirements:

- Minimum 13 characters long when set by a human.
- Minimum 13 characters long minimum when set by a system/service.
- The system must support a password of at least 64 characters maximum length.
- All ASCII characters (including space) shall be supported for passwords.
- The password shall not be truncated when processed.
- The chosen password shall be checked with known password dictionaries.

- The system shall allow the number of password attempts before lockout to be set (5.1.2.8 refers).
- The system shall deny the repeated use or recycling of the last five passwords.
- here shall be no complexity requirements for passwords.
- There shall be no password expiration period.
- There shall be no password hints.
- There shall be no knowledge-based authentication (e.g. who was your best friend in high school?).

5.1.4.3 Passwords shall not be stored, electronically or hard copy, in plain text. The exception to this requirement is the sharing of an initial or recovery password with an authorised user, which must be in a separate communication to the user identification.

5.1.4.4 Copies of root, administrator, and system account details, retained for emergency use, must be stored separately from the system and in a secure storage.

Note: For safety critical and service critical systems the following additional requirements shall apply:

5.1.4.5 Password generation and lifetime restrictions for human users

5.1.4.6 Password lifetime restrictions for all users

5.1.5 Wireless Access Management

As an organisation, TfL must ensure that the control system provides the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.

The system owner must ensure compliance with the following minimum baseline requirements:

5.1.5.1 Maintain the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.

5.1.5.2 Wireless networks shall have MAC Address filtering enabled.

5.1.5.3 Maintain the capability to authorise, monitor and enforce usage restrictions for wireless connectivity to the control system.

5.1.5.4 Wireless systems shall employ a key management system.

5.1.5.5 Wireless encryption requirements are contained in Section 5.5.5 (Encryption).

5.1.5.6 Wireless devices shall be protected with security controls, such as access control and encryption, to protect the devices from unauthorised access, modification, or use.

5.1.5.7 Where Public Key Infrastructure (PKI) is utilised, maintain the capability to operate a PKI according to commonly accepted best practices or obtain public key certificates from an existing PKI.

Requirements 5.1.5.8 and 5.1.5.9 are only applicable to systems that provide open public WIFI networks at Stations and on passenger trains or trams.

5.1.5.8 There shall be a process to disable open public WIFI networks within 15 minutes of being requested.

5.1.5.9 There shall be a process to reenable open public WIFI networks

Note: For safety critical and service critical systems the following additional requirements shall apply:

5.1.5.10 Hardware security for public key authentication

5.1.6 User Change Management and Access Review

As an organisation, TfL must ensure they are able to track joiners, movers and leavers in order to ensure that each individual user is only granted minimum required access rights for their role, that these rights are reviewed when they change role and revoked on leaving TfL.

It is essential that access to any OT system which supports the delivery of TfL services is authorised by the system owner or a delegated deputy (Section 5.1.1.1 refers).

System owners should conduct a regular review of user access rights for the system(s) they are responsible for and ensure those which are no longer required are revoked (Sections 5.1.1.3 and 5.1.1.4 refer).

System owners must conduct user change management and access review activities through the following minimum baseline requirements:

5.1.6.1 All human users shall be uniquely identified and authenticated.

5.1.6.2 All non-human users shall be uniquely identified and authenticated.

5.1.6.3 This identification and authentication shall be enforced on all interfaces which provide access to the control system to support the verification of the principle of least privilege.

5.1.6.4 The management of all accounts including adding, activating, modifying, disabling, and removing accounts is to only be performed by authorised users.

5.1.6.5 Users are to be managed through the use of identifiers by user, group, role, or control system interface.

5.1.6.6 Ensure to:

- change all default authenticators upon control system installation.
- change/refresh all authenticators as required; and
- protect all authenticators from unauthorised disclosure and modification when stored and transmitted.

5.1.7 Monitor Access

As an organisation, TfL must provide the capability to log and monitor all user access to any OT system, which will form an integral element of system monitoring.

The system owner must maintain compliance with the following minimum baseline requirements:

5.1.7.1 Feedback on authentication information during the authentication process shall be obscured. (For example, responding to a failed login attempt with a “login failed” message rather than “your password was incorrect” which shows an attacker they have used a valid user ID).

5.1.7.2 There shall be an enforced limit, currently three (Section 5.1.2.8 refers), of consecutive invalid access attempts for any user (human, software process or device) during a configurable time period, which is recommended to be set at thirty minutes.

5.1.7.3 Any user shall be denied access for three hours or until unlocked by an administrator when the consecutive invalid access attempts limit has been exceeded (Section 5.1.2.8 refers).

5.1.7.4 There shall be the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorised personnel.

5.1.7.5 The capability shall be maintained to enforce authorisations assigned to all users (humans, software processes and devices) for controlling use of the system to support segregation of duties and least privilege.

5.1.7.6 The capability shall be maintained for an authorised user or role to define and modify the mapping of permissions to roles for all human users, software processes and devices.

5.1.7.7 The capability shall be maintained to automatically enforce configurable usage restrictions that include:

- preventing the use of portable and mobile devices
- restricting code and data transfer to/from authorised portable and mobile devices.

5.1.7.8 The capability to log the following events shall be maintained:

- Failed log in attempts
- Automatic account reset
- Administrative account reset
- Successful logins out of normal working patterns
- Password changes
- Permission changes
- Failed attempts to connect unauthorised portable and mobile devices
- Connection of authorised portable and mobile devices.

5.1.7.9 The capability shall be maintained to forward user logging securely to a central log collector (Section 6 refers).

5.2 Data Security

TfL must protect data which is stored or transmitted electronically from actions such as unauthorised access, modification or deletion that may cause an adverse impact on essential functions.

This protection must be underpinned by a good understanding of the data that is important to the delivery of the TfL services, where it is stored, where it travels, and how unavailability or unauthorised access, modification or deletion would impact the service. This also applies to any third parties storing or accessing data important to the delivery of TfL services.

5.2.1 Identify and Understand Critical Data (Information and Documents)

As an organisation, TfL must ensure that for each OT system, there is a record of the location, type, quantity, and quality of data important to the delivery of TfL services. In addition, this record must include the context, limitations and dependencies of the data that is critical to TfL services.

Much of the information about the OT system may be stored electronically or in hardcopy outside the system and is not protected by OT authorisation controls. Unauthorised access and use of this information are a threat to OT security and this information needs to be appropriately controlled and managed.

The system owner must ensure compliance with the following minimum baseline requirements:

5.2.1.1 A document management process shall be maintained for OT information which supports the system.

5.2.1.2 Information classification levels, commensurate with S1782 Information Security Classification, shall be implemented for access and control, including sharing, copying, transmitting, and distributing of OT information.

5.2.1.3 All logical assets within the scope of the system (including, but not limited to, system design information, vulnerability assessments and network diagrams) shall be classified to indicate the protection required commensurate with the consequence of compromise. (S1782 – Information Security Classification refers).

5.2.1.4 Implement and maintain procedures, commensurate with S1782 Information Security Classification, for retention, physical and integrity protection, destruction, and disposal of all assets based on their classification, including written and electronic records, equipment and other media containing information, with consideration for legal or regulatory requirements.

5.2.1.5 Measures shall be employed to ensure long-term records can be retrieved. This could include converting the data to a newer format or retaining older equipment that can read the data.

5.2.1.6 Information that requires special control or handling shall be reviewed on a periodic, at least annual, basis to validate that special handling is still required.

5.2.1.7 Periodic, minimum annually, reviews of compliance to S1782 Information Security Classification shall be performed.

5.2.2 Understand Data Links

As an organisation, TfL must ensure that for each OT system, there is a documented and up to date understanding of the data links used to transmit data that is critical or important to the delivery of TfL services.

The system owner must ensure compliance with the following minimum baseline requirements:

5.2.2.1 A documented record must be maintained of all the data links that transfer data into or out of the system.

5.2.2.2 The record must include the context, limitations and dependencies of the data links that are critical to TfL services.

5.2.2.3 The record shall support and inform the capability to protect the integrity of transmitted information (Section 5.5.2 refers).

5.2.3 Identify Mobile Devices and Portable Media

As an organisation, TfL must ensure that all mobile devices and media that may hold data important to the delivery of the TfL services and are used to support the OT system must be identified and recorded.

Mobile devices include but is not limited to laptop computers and handheld programmers. Media assets include removable media and devices such as floppy disks, CDs, DVDs, and USB memory sticks, as well as printed reports and documents.

If an adversary gains access to backup media associated with an OT system, it could provide valuable data for launching an attack. Recovering an authentication file from the backups might allow an adversary to run password cracking tools and extract usable passwords. In addition, the backups typically contain machine names, IP addresses, software version numbers, usernames, and other data useful in planning an attack.

The system owner must ensure compliance with the following minimum baseline requirements:

5.2.3.1 The use of any unauthorised mobile device or portable media on any node that is part of or connected to the OT system shall not be permitted in order to prevent the introduction of malware or the inadvertent loss or theft of data.

5.2.3.2 Systems shall only use removable media and mobile devices where absolutely necessary and must undergo business justification and further risk assessment to provide justification for all enabled USB ports, CD/DVD drives and other removable media devices.

5.2.3.3 Where the use of a mobile device or portable media is permitted, this must be a dedicated device which is subject to an equivalent level of protective controls to the OT system that it is used to support.

5.2.3.4 There shall be a documented process to verify that a mobile device is free from malware before and after it is connected to the system (Section 5.7.1 refers).

5.2.3.5 A documented record of all authorised mobile devices and portable media which are associated with the system must be maintained.

5.2.3.6 The number of authorised removable media and mobile devices shall be kept to the absolute minimum required for system operation.

5.2.3.7 Mobile devices and portable media that will be transported between physically secure locations is to employ data at rest encryption.

5.2.3.8 Where the use of removable media is authorised and the system supports it, software shall be used to enforce removable media processes.

5.2.3.9 Mobile devices and portable media are to be secured in a locked cabinet when not in use.

5.2.3.10 Periodic reviews of compliance, minimum six-monthly, of the record of all authorised mobile devices and portable media.

5.2.3.11 Implement and maintain procedures for the actions to be taken due to the loss of mobile devices and portable media.

5.2.4 Manage Data Holdings

As an organisation, TfL must ensure that data holdings relating to OT are managed throughout the life of the system.

The system owner must ensure compliance with the following minimum baseline requirements:

5.2.4.1 A documented record shall be maintained of data holdings relating to the system which will include, but not be limited to, design documentation, operational data, system logs and backups.

5.2.4.2 Review and then remove or minimise unnecessary copies or unneeded historic data.

5.2.4.3 Data retention must be aligned to regulation, system operating requirements and security monitoring requirements. For example, if system logs are ingested into a centralised logging system, they do not need to be retained in perpetuity on the system, but only for local fault finding or recovery purposes, which would require up to a months' worth of data.

5.2.4.4 Periodic reviews of compliance, minimum six-monthly, of the record of all data holdings.

5.2.4.5 Data which is no longer required or has passed its retention period shall be deleted or destroyed in a secure manner.

5.3 Personnel Security

TfL must closely manage privileged user access to networks and information systems supporting the TfL services.

Personnel security has three related aspects. From an organisational HR perspective, it involves looking at new and current personnel to determine if they will maintain the OT security for the organisation. For new personnel, the personnel security process evaluates them prior to their entry into the organisation making sure they demonstrate behaviours consistent with their future security responsibility. For current personnel, the personnel security process establishes that they continue to demonstrate behaviour consistent with their current security responsibilities.

Personnel security requirements are also driven by concerns about training, approved staff, awareness of the system, awareness of safety and in some instances malicious activity (generally referred to as Insider Threats). For more information on Insider Threats refer to G1134: Personnel Security – Insider Threat.

From a system owner perspective, the approach is ensuring that the system has the required capabilities and processes to support the minimum baseline controls for personnel security and builds on the baseline identity and access control requirements in Section 5.1.

5.3.1 Privileged User Access

TfL must ensure that individuals who require privileged levels of user access receive additional validation and authentication.

The system owner must ensure compliance with the following minimum baseline requirements:

5.3.1.1 Privileged access shall be granted, changed, or terminated on the authority of an appropriate senior manager or system owner.

5.3.1.2 Privileged access accounts should be dedicated to a specific function and must not be used for general administrative tasks.

5.3.1.3 Privileged access accounts must use MFA.

5.3.1.4 A non-privileged user must not be able to gain privileged access rights without proper authorisation and such authorisation should only be temporary to support an urgent business need.

5.3.1.5 Enforce authorisations assigned to all users (humans, software processes and devices) for controlling use of the system to support segregation of duties and least privilege.

5.3.1.6 An authorised user or role shall maintain and modify the mapping of permissions to roles for all human users.

5.3.2 User Management

TfL must ensure that the identities of the individuals, whether employees or partners, with privileged access to networks and information systems to support the TfL services systems are known and managed.

The system owner must ensure compliance with the following minimum baseline requirements:

5.3.2.1 A record shall be maintained of all privileged access accounts, including details of the individual(s) and devices authorised to use the account, their permissions, and the authorising manager.

5.3.2.2 Privileged access accounts shall be suspended or removed immediately when they are no longer needed, for example in the event of a job change.

5.3.2.3 The capability to automatically enforce configurable usage restrictions for users shall be maintained, which includes:

- preventing the use of portable and mobile devices
- requiring context specific authorisation; and

MAYOR OF LONDON
Transport for London
TfL RESTRICTED

- restricting code and data transfer to/from portable and mobile devices.

5.3.2.4 Implement and maintain procedures for the creation, distribution, management and administration of privileged user accounts.

Note: For safety critical and service critical systems the following additional requirements shall apply:

5.3.2.5 Supervisor override

5.3.2.6 Hardware security for public key authentication.

5.3.3 Role Based Access

TfL should ensure that privileged users are granted only specific privileged permissions which are essential to their business role or function.

The system owner must ensure compliance with the following minimum baseline requirements:

5.3.3.1 Duties should be segregated amongst personnel to maintain appropriate checks and balances, so that no single individual has total control over actions that change the functional operation of the OT.

5.3.3.2 Personnel should be assessed for the critical positions controlling and maintaining the OT.

5.3.4 Privileged Access Review

TfL must conduct a regular review and validation of activity by privileged and standard users to identify any unauthorised or unusual activities.

The system owner must ensure compliance with the following minimum baseline requirements:

5.3.4.1 All established privileged access accounts shall be reviewed monthly to ensure that the accounts only provide the minimum required permissions and remain a valid requirement for operating the system.

5.3.4.2 Maintain audit records relevant to privileged account security for the following categories:

- access control
- request errors
- operating system events
- system events
- configuration changes
- potential reconnaissance activity and audit log events.

5.3.4.3 Individual audit records shall include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result.

5.3.4.4 Maintain sufficient audit record storage capacity for log management and system configuration. This shall be to a minimum of one year's worth of records.

5.3.4.5 Maintain timestamps for use in audit record generation.

Note: For safety critical and service critical systems the following additional requirements shall apply:
5.3.4.6 Supervisor override
5.3.4.7 Hardware security for public key authentication.

5.4 Physical Security

TfL must ensure that physical security arrangements compliment OT Cyber Security and protect the OT supporting the TfL services from direct attack.

This will create a secure environment for the protection of OT assets.

This section should be read in conjunction with established physical security standards (Listed or linked in Section 13) and in consultation with the physical security team. The intention is to ensure that physical and Cyber Security arrangements are complementary and maintained properly throughout the life of the system. This section is not intended to replace established physical security standards, but rather to highlight to TfL staff and partners where particular physical security considerations are relevant to OT systems.

Surveillance and security systems, in particular CCTV, access control systems and intruder detection systems shall comply with S1147 Surveillance and Security Systems.

An asset is any physical or logical object owned by, or operated by, TfL having either a perceived or actual value to the organisation for delivery of TfL services. OT assets are those assets that are a part of the OT, either physical or cyber or that can affect the operation of the OT.

IT assets used in support of or as part of OT systems shall comply with S1747 Physical Security of IT Equipment.

Physical security measures ensure that all assets, specifically those related to the OT of an organisation, are protected physically from unauthorised access, loss, damage, misuse, and the like. Environmental security measures ensure that the assets of an organisation are protected against environmental conditions that would make them unusable or damage the information they contain.

Physical and environmental security measures should be maintained to complement the Cyber Security measures taken to protect assets that are part of the OT and coordinated with the physical security of the remainder of the infrastructure.

It is important to include all systems in the scope and not just limit the effort to traditional computer room facilities and equipment rooms. Practical engineering judgment should be used to balance the risks when determining physical security procedures.

Physical segmentation is a key security countermeasure designed to compartmentalise devices into security Zones where identified security practices are employed to achieve the desired target security level.

The physical protection of the cyber components and data associated with the system must be addressed as part of the overall security of a system. Security at many OT facilities is closely tied to site safety. A primary goal is to keep people out of hazardous situations without preventing them from doing their job or carrying out

emergency procedures. Physical security controls are any physical measures, either active or passive, that limit physical access to any information assets in the OT environment.

These measures are employed to prevent many types of undesirable effects, including:

- Unauthorised physical access to sensitive locations
- Physical modification, manipulation, theft or other removal, or destruction of existing systems, infrastructure, communications interfaces, personnel, or physical locations
- Unauthorised observation of sensitive informational assets through visual observation, note taking, photographs, or other means
- Prevention of unauthorised introduction of new systems, infrastructure, communications interfaces, or other hardware
- Prevention of unauthorised introduction of devices intentionally designed to cause hardware manipulation, communications eavesdropping, or other harmful impact.

The system owner must ensure compliance with the following minimum baseline requirements:

5.4.1.1 Security procedures that address the physical security in the protection of assets shall be implemented and maintained for the system

5.4.1.2 At least one physical security perimeter shall be maintained to provide barriers against unauthorised access to protected assets. Critical components and systems must have at least two physical perimeters.

5.4.1.3 There must be entry controls at each physical barrier or boundary.

5.4.1.4 There shall be an auditable record of access to equipment via a security barrier or boundary.

5.4.1.5 All connections under the control of the system shall be adequately protected from tampering or damage.

5.4.1.6 Arrangements must be established to protect assets against environmental damage from threats such as fire, water, smoke, dust, radiation, corrosion, and impact.

5.4.1.7 Maintenance procedures must be implemented for all equipment assets, including auxiliary environmental equipment, to ensure proper operation through correct maintenance.

5.4.1.8 Implement and maintain procedures for monitoring, alarming and investigating when physical or environmental security is compromised.

5.4.1.9 Procedures should be implemented and audited with respect to the addition, removal, and disposal of all assets.

5.4.1.10 Implement and maintain procedures to ensure the protection of critical components during the interruption of operations, for example, due to fire, water ingress, security breach, interruption, natural or any other type of disaster.

5.4.1.11 Physical security arrangements must be reviewed on a six-monthly basis.

5.5 Network Security

TfL must ensure that the transit of data important or critical to the delivery of TfL services is protected. This includes the transfer of data to third parties.

5.5.1 Data Transfer

The system owner must ensure that:

5.5.1.1 All Conduits for data transfer have been identified according to Section 5.2.2.

5.5.1.2 Conduits shall be maintained to protect the data they are transferring. Options to protect the data include, but are not limited to:

- Encryption (See Section 5.5.5)
- Secure Tunnelling, such as VPNs (See Section 5.5.6)
- Data Diodes
- Inbound and outbound boundary (firewall) rules.

5.5.2 Data Protection

TfL must ensure that the system has the capability to protect the integrity of transmitted information.

The system owner must ensure compliance with the following minimum baseline requirements:

5.5.2.1 Maintain confidentiality of information for which explicit read authorisation is supported, whether at rest or in transit.

Staff and partners should pay particular attention to the information confidentiality relating to portable and mobile devices (for example engineering laptops and USB sticks).

5.5.2.2 Authentication information, such as passwords, should be considered confidential, and never be sent in a readable format.

5.5.2.3 The confidentiality of information at rest shall be protected.

5.5.2.4 Communications over untrusted or open networks shall be encrypted (See Section 5.5.5 Encryption for details).

5.5.2.5 Maintain the protection of the confidentiality of remote access sessions traversing an untrusted network.

Note: Encryption is a common mechanism for ensuring information confidentiality.

5.5.3 Single Points of Failure

TfL must ensure that the system has been designed to eliminate single points of failure where possible.

The system owner must ensure compliance with the following minimum baseline requirements:

5.5.3.1 As part of the handover process, the project must have identified single points where, due to failure, there is a significant risk of impact on the delivery of the TfL services.

5.5.3.2 Where possible, these single points of failure should have been eliminated during the design stages, but if this is not achievable, this must be recorded in the project/system risk register and incorporated into any response plans for the system.

5.5.4 Resilient Communications

TfL must ensure there are alternative communication paths where there is a significant risk of impact on the delivery of TfL services if a primary communication path is lost or interrupted.

The system owner must ensure compliance with the following minimum baseline requirements:

5.5.4.1 Communication paths where, due to failure, may have a significant risk of impact on the delivery of the TfL services must be documented, reviewed annually and compensating procedures established.

5.5.4.2 Alternative communication paths to eliminate the risk to service delivery in the primary path is lost or interrupted shall be maintained and tested. If an alternative path cannot be established, this shall be recorded in the system risk register and highlighted in any response plans for the system.

5.5.5 Encryption

TfL must ensure that the system has capability to protect the integrity of transmitted information.

This section provides the specific requirements for different methods of encryption, but it should also be noted that depending on the location or design of the system in question, alternative controls could be adopted.

The selected encryption method must provide a commensurate level of protection for the data, both at rest and in transit. This protection will be in line with the impact on TfL services if the data is compromised and will most likely have been informed by a risk or impact assessment, so the emphasis is on maintaining the level of protection through the life of the system.

Depending on the type of encryption, the system owner must ensure compliance with the following minimum baseline requirements:

5.5.5.1 For Private Key Encryption (Symmetric Key Cipher), a minimum of AES-256 must be used.

5.5.5.2 For stream ciphers, RC4 and algorithms derived from that shall not be used. AES may be used in a cryptographic mode that allows streaming provided that the key is changed in accordance with the limitations of the cryptographic mode chosen. Keys for streaming cipher modes of operation must only be used for one stream and shall not be reused.

5.5.5.3 The Electronic Codebook (ECB) and Cypher Block Chaining (CBC) block cipher mode of operation must not be used.

5.5.5.4 For key exchange, the DH (Diffie-Hellmann) algorithm must be used with a key length of at least 3072-bit (Group 15). Ephemeral Diffie-Hellmann is preferred.

5.5.5.5 For Public Key Infrastructure (Asymmetric Key Ciphers) encryption, the RSA algorithm with a key length of at least 3072-bit must be used.

5.5.5.6 For Public Key Infrastructure (Asymmetric Key Ciphers) authentication, RSA or DSA algorithms with a key length of at least 3072-bit must be used.

> DSA was originally designed for digital signatures and not for general encryption, although it can be used for general encryption purposes. NIST is trying to deprecate DSA in favour of Elliptic-Curve DSA (ECDSA) and Edwards Curve DSA (EdDSA).
>
> Consideration should be given to Elliptic Curve Cryptography (ECC) instead of RSA, such as Elliptic Curve Diffie Hellmann, since for a given approved curve, the key length is roughly halved to get the same strength of encryption.

5.5.5.7 For data hashing, SHA-256 must be used as minimum. SHA3 shall also be allowed as well as SHA2, with more than 256 bits (FIPS 202).

5.5.5.8 For file integrity checking, SHA-2 must be used as a minimum. SHA3 shall also be allowed as well as SHA2, with more than 256 bits (FIPS 202).

5.5.5.9 For 802.11-based infrastructure, WPA2 Enterprise with AES CCMP encryption and EAP-TLS 1.2 must be used as a minimum.

5.5.5.10 All encryption keys must be changed from their default value before use.

5.5.5.11 All encryption keys must be randomly generated, not human-specified; except for file-level encryption passwords specified by individual users.

5.5.5.12 Cryptographically Secure Pseudorandom Number Generators (CSPRNGs) must be used to generate encryption keys and the following CSPRNGs should be used where possible:

- RNGCryptoServiceProvider, CryptGenRandom, FIPSGenRandom or RtlGenRandom (Microsoft Windows XP Service Pack 3 or later only).
- /dev/random, /dev/urandom or /dev/arandom (preferred) (*nix-based systems).
- Any other Evaluation Assurance Level (EAL) 4+ accredited CSPRNGs.
- Any other Federal Information Processing Standard (FIPS) 186-2 compliant CSPRNGs.

5.5.5.13 CSPRNGs based on the following functions are deemed insecure and must not be used:

- Rand()
- Math.Random()

5.5.5.14 Symmetric and Private keys must be stored securely at rest using PKCS#11 or PKCS#12.

5.5.5.15 Encryption hardware should be certified to FIPS 140-2 (tamper evident) as a minimum.

5.5.5.16 Encryption hardware should be protected from physical tampering and uncontrolled electronic connections.

Cryptography also introduces key management issues since robust security policies require periodic key changes. This process becomes more difficult as the geographic size of the OT increases, with extensive OT systems being the most severe example. As site visits to change keys can be costly and slow, it is useful to be able to change keys remotely.

Note: For safety critical and service critical systems the following additional requirements shall apply: 5.5.5.17 Cryptographic integrity protection.

5.5.6 Virtual Private Networks (VPN)

TfL must ensure that any VPN used to encrypt communications is configured securely.

The system owner must ensure compliance with the following minimum baseline requirements:

5.5.6.1 When a VPN is implemented use one of the following protocols:

- Internet Protocol Security (IPsec)
- Transport Layer Security (TLS).

5.5.6.2 For remote access connections, the VPN shall include a logical break point (jump server) at an OT De-Militarised Zone (DMZ) to allow the link to be monitored.

5.5.7 Backups

TfL must ensure that there are backups of the data required to restore systems to normal operational capability (See also Section 7.2).

The system owner must ensure compliance with the following minimum baseline requirements:

5.5.7.1 Maintain secured backups of the data (systems, software, licenses, configurations, data, and other relevant information) required to allow the TfL services to operate or to restore the TfL services to an operational state within an acceptable timeframe.

Note: Automated backups are recommended to ensure that all required files are captured with reduced operator overhead.

5.5.7.2 The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be maintained without affecting normal operations.

5.5.7.3 Although not usually required for system recovery, information required for post-incident forensic activity (for example, audit logs) should be specifically included in the backup.

5.5.7.4 Where a backup contains confidential information, encryption should be considered where this will not affect any recovery operations, or the backup should be secured in a suitable lockable storage or safe.

5.5.7.5 Maintain the capability for backups to be extracted and stored securely in a separate location.

5.5.7.6 Full-bit images shall be recorded as configuration baselines for operational systems and assets. These images must be stored securely.

5.5.7.7 Verify the reliability of backup mechanisms, including the capability to conduct routine tests, at least 6-monthly, to ensure the backup process is functioning correctly and that the backups are usable.

5.5.7.8 The backups shall be accessible if an extreme event occurs.

5.5.7.9 Develop, implement and maintain procedures for the testing and verification of backups.

5.6 System Security

TfL must ensure that security is designed into the network and information systems that support the delivery of TfL services from the outset.

Staff and partners should recognise that secure design principles have been adopted to minimise the attack surface and ensure that the delivery of the TfL services should not be impacted by the exploitation of any single vulnerability. Actions taken during operations and maintenance should maintain, as a minimum, or improve, where possible, that secure envelope.

This section should be read in conjunction with the Purdue Model and secure OT architecture paragraphs in Section 4.

5.6.1 Secure by Design

TfL must employ appropriate expertise to design secure networks and information systems supporting the TfL services.

The system owner must ensure compliance with the following minimum baseline requirements:

5.6.1.1 The integrity of transmitted information shall be protected (Section 5.5 refers).

5.6.1.2 Only permitted, verified, and tested software from authorised sources shall be installed.

5.6.1.3 Port security shall be implemented on network devices to prevent the use of unused ports.

5.6.1.4 There shall be no unmanaged network devices on the system

5.6.1.5 Protection mechanisms shall be employed to prevent, detect, report, and mitigate the effects of malicious code or unauthorised software.

5.6.1.6 The protection mechanisms shall be updated on at least a quarterly basis or when an update is provided by the manufacturer.

5.6.1.7 Verify the intended operation of the security functions on a periodic basis and report when anomalies are discovered during verification and scheduled maintenance. These security functions shall include all those necessary to support the security requirements specified in this standard.

5.6.1.8 Detect, record, report and protect against unauthorised changes to software and information at rest.

5.6.1.9 Maintain the system so that it validates the syntax and content of any input which is used as an input that directly impacts the action of the system.

5.6.1.10 Maintain the systems capability to set outputs to a predetermined state if normal operation cannot be maintained because of an attack.

5.6.1.11 Maintain the systems capability to identify and handle error conditions in a manner such that effective remediation can occur. This shall be done in a manner which does not provide information that could be exploited by adversaries to attack the OT unless revealing this information is necessary for the timely troubleshooting of problems.

5.6.1.12 Maintain the systems capability to protect the integrity of sessions.

5.6.1.13 Maintain the systems capability to reject invalid session IDs.

5.6.1.14 Maintain the protection of audit information and audit tools (if present) from unauthorised access, modification, and deletion.

5.6.1.15 The number of concurrent sessions per interface for any given user (human, software process or device) shall be limited to a configurable number of sessions.

5.6.1.16 Malicious code protection mechanisms shall be maintained at all entry and exit points.

5.6.1.17 The partitioning of data, applications and services based on criticality to facilitate implementing a zoning model (Section 5.6.5 and supporting guidance refers) shall be maintained.

5.6.1.18 Maintain the systems capability to operate in a degraded mode during a Denial of Service (DoS) event.

5.6.1.19 Maintain the systems capability to manage communication loads (such as using rate limiting) to mitigate the effects of information flooding types of DoS events.

5.6.1.20 Maintain the systems capability to limit the use of resources by security functions to prevent resource exhaustion.

Note:	For safety critical and service critical systems the following additional requirements shall apply:
5.6.1.21	Central management and reporting for malicious code protection.
5.6.1.22	Automated mechanisms for security functionality verification.
5.6.1.23	Security functionality verification during normal operation.

5.6.1.24	Automated notification about integrity violations.
5.6.1.25	Hardware and software inventory.
5.6.1.26	Discovery tooling.
Note: Where these has been implemented they shall be maintained.	

5.6.2 Configuration Management / Change Control

TfL must implement configuration management processes to control modifications to hardware, firmware, software, and documentation to ensure that the system is protected against improper modifications prior to, during, and after system implementation.

The system owner must ensure compliance with the following minimum baseline requirements:

5.6.2.1 The current OT network configuration and device configurations must always be known and documented.

5.6.2.2 A formal change management process shall be used to ensure that all modifications to an OT network meet, or exceed, the security requirements as defined in the system specifications or low-level design.

5.6.2.3 Risk assessment must be performed on all changes to the OT network that could affect security, including configuration changes, the addition of network components, and installation of software.

5.6.2.4 There should be restricted access to configuration settings of OT components.

5.6.3 System and Information Integrity

TfL must maintain system and information integrity to ensure that sensitive data has not been modified or deleted in an unauthorised and undetected manner.

The system owner must ensure compliance with the following minimum baseline requirements:

5.6.3.1 There shall be controls maintained for malware detection, spam and spyware protection and intrusion detection.

5.6.3.2 An alert shall be investigated if these controls are triggered.

5.6.4 Malware Detection

TfL must ensure that malware detection products are deployed as widely as possible.

Malware detection products evaluate files on a computer's storage devices against an inventory of known malware signature files.

Anti-malware software can be deployed on workstations, servers, firewalls, and handheld devices, but may not be appropriate for operational devices.

Anti-malware tools only function effectively when installed, configured, running full-time, and maintained properly against the state of known attack methods and payloads.

The system owner must ensure compliance with the following minimum baseline requirements:

5.6.4.1 Anti-malware products must be maintained on all devices that can support it. This includes, but is not limited to, Windows, Unix, Linux systems, etc. used as consoles, engineering workstations, data historians, HMIs and general-purpose SCADA and backup servers.

5.6.4.2 Malware detection shall be maintained be this anti-malware protection and / or whitelisting. Whitelisting must:

- Prevent the execution of all unauthorised software.
- Provide an alert when unauthorised software attempts to run.
- Report the list of authorised software and versions that are on the OT assets.

5.6.4.3 Signatures and updates for anti-malware products installed on the OT Network must only be obtained from secure sources (i.e. a dedicated anti-malware distribution server, located within a DMZ outside the OT network (Section 5.6.5 refers)).

5.6.4.4 Anti-malware tools and updates shall be verified that their use does not impact system performance.

5.6.4.5 Malware protection shall be in place at all physical and logical network entry and exit points, which may also need the use of 'Sheep Dips'.

5.6.4.6 Tested and verified anti-malware tool updates and signatures must be applied at least once every 4 weeks.

5.6.4.7 Implement and maintain procedures for the for the test and implementation of anti-malware signatures and updates.

5.6.5 Network Segmentation

5.6.5.1 TfL must ensure that the networks and information systems supporting the TfL services are segregated into appropriate security Zones as defined in the Zone and Conduit model (See Section 4.6 of the supporting Guidance document).

Network segmentation and the level of protection it provides will vary greatly depending on the overall network architecture. Logically segmenting networks based on their functionality provides some measure of protection but may still lead to single-points-of-failure if a network device is compromised. Physically segmenting networks provides another level of protection by removing that single-point-of-failure case but will lead to a more complex and costly network design.

5.6.5.2 The system shall be handed over with the following requirements and the System owner must ensure these are maintained throughout the operational lifecycle of the system:

5.6.5.3 The system design shall group key OT devices into separate Zones with common security levels to manage security risks and to achieve a desired target security level for each Zone.

5.6.5.4 The system shall be separated into Zones and each Zone shall have a clearly defined security level.

5.6.5.5 There shall be enforced Conduits between Zones.

5.6.5.6 There shall be firewalls between Zones of differing security levels and firewall rules shall be reviewed at least every 12 months.

5.6.5.7 There shall be Access Control Lists (ACLs) between Zones of common security levels, which shall be reviewed at least every 12 months.

5.6.5.8 There shall be a DMZ between the IT and OT Networks.

5.6.5.9 There shall be no direct Internet access to or from the OT Network.

5.6.5.10 An OT DMZ shall be used for all outbound connectivity.

5.6.5.11 There shall be Virtual Local Area Networks (VLANs) to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.

5.6.5.12 The design shall ensure there are simple data flows between systems, devices, and interfaces to enable effective monitoring.

5.6.5.13 Any connections to external networks or other systems must occur through managed interfaces consisting of appropriate boundary protection devices (for example, proxies, gateways, routers, firewalls, unidirectional gateways, guards and encrypted tunnels) arranged in an effective architecture (for example, firewalls protecting application gateways residing in a DMZ). These connections must be necessary for operational and business purposes and subject to risk assessment.

5.6.5.14 High-risk or critical systems shall be subject to a risk assessment to determine if they should be isolated from or employ a barrier device to separate them from other Zones with different security levels or risks i.e. unidirectional gateways.

5.6.5.15 The system shall provide the capability to support partitioning of data, applications and services based on criticality to facilitate the zoning model. This may require that some servers may need to be duplicated on the control system network to support normal network features, for example dynamic host configuration protocol (DHCP), domain name service (DNS) or local certificate authorities (CAs).

5.6.5.16 Systems shall only be connected to external networks where absolutely necessary and must undergo business justification and further risk assessment to provide justification.

Note:	For safety critical and service critical systems the following additional requirements shall apply:
5.6.5.17	Independence from non-control system networks.
5.6.5.18	Greater logical and physical isolation of critical networks.
5.6.5.19	Island mode (physical isolation of critical networks).
5.6.5.20	Fail close operation.
5.6.5.21	Uni-directional gateways or data diodes.

5.6.6 Zone boundary protection

TfL must ensure that the system shall provide the capability to monitor and control communications at Zone or segmentation boundaries to enforce the compartmentalisation defined in the Zone and Conduits model.

The system owner must ensure compliance with the following minimum baseline requirements:

5.6.6.1 Maintain the systems capability to monitor and control communications at Zone boundaries.

5.6.6.2 Maintain the systems capability to deny network traffic by default and allow network traffic by exception (also termed deny all, permit by exception).

5.6.6.3 In response to an incident, it may be necessary to break the connections between different network segments. In that event, the services necessary to support essential operations should be maintained in such a way that the devices can continue to operate properly and/or shutdown in an orderly manner.

5.6.6.4 System boundary protections at any designated alternate location should provide the same levels of protection as that of the primary site.

5.6.7 General purpose person-to-person communication restrictions

5.6.7.1 TfL shall ensure that the system shall provide the capability to restrict or prevent general purpose person-to-person messages from being received from users or systems external to the system.

5.6.7.2 The system owner must ensure compliance with the following minimum baseline requirements:

5.6.7.3 Maintain the systems capability to restrict email or other messaging solutions that provide internal computer-to-external computer communications using outbound messages.

These internal-to external communications may be limited to the purpose of sending system alerts or other computer-generated information messages to users or systems external to the system.

5.6.7.4 Maintain the systems capability to utilise preconfigured messages to transmit alert or status information.

5.6.7.5 Maintain the systems capability to not allow users to attach files or other information to these outbound-only messages at the time the messages are created by the system.

Note: For safety critical and service critical systems the following additional mitigations shall apply:

5.6.7.6 Prohibit all general-purpose person-to-person communication.

5.6.8 Security configuration settings

TfL shall ensure that the system has the capability to be configured according to recommended security configurations (See Section 5.6.9).

The system owner must ensure compliance with the following minimum baseline requirements:

5.6.8.1 Maintain the systems interface that supports the management of network and security configuration settings.

5.6.8.2 Maintain the systems capability to support monitoring and control of changes to the configuration settings.

Note: For safety critical and service critical systems the following additional requirements shall apply:

5.6.8.4 Implementation of an automated check process where the current security settings are automatically collected by an agent and compared to approved settings, with changes being alerted.

5.6.9 Secure Configurations

TfL shall ensure that the system has been configured according to recommended network and security configurations, aka system hardening.

If the manufacturer's recommended configurations are different to any configurations required by this standard, the differences must be reviewed and the most restrictive configuration applied, unless this would impact the safe and reliable operation of the system.

The system owner must ensure compliance with the following minimum baseline requirements:

5.6.9.1 There shall be documentation maintained which details all applications, utilities, system services, scripts, configuration files, databases, and all other software required and the appropriate configurations, including revisions and/or patch levels for each of the computer systems associated with the system.

5.6.9.2 There shall be a documented list of services required for any computer system running control system applications or required to interface the control system applications. The list must include:

- All ports and services required for normal operation as well as any other ports and services required for emergency operation.
- Justification as to why each service is necessary for operation.

5.6.9.3 All software components that are not required for the operation and maintenance of the control system must have been removed prior to operation and shall not be restored during operations. This must include, but is not limited to:

- Games
- Device drivers for network devices not in use
- Instant messaging services
- Servers or clients for unused Internet services
- Software compilers in all user workstations and servers except for development workstations and servers
- Software compilers for languages that are not used in the control system
- Unused networking and communications protocols

- Unused administrative utilities, diagnostics, network management, and system management functions
- Backups of files, databases, and programs used only during system development
- All unused data and configuration files
- Sample programs and scripts
- Unused document processing utilities (Microsoft Word, Excel, PowerPoint, Adobe Acrobat, OpenOffice, etc.).

5.6.9.4 Unnecessary credentials shall be removed (preferred option) or disabled.

5.6.9.5 Unnecessary communication ports and media drives shall remain disabled by logical (software) or physical (disconnection) means or secured with an engineered barrier.

5.6.9.6 The system BIOS shall remain password protected to prevent unauthorised configuration changes, unless this is not technically possible, which must be recorded in the system risk register.

5.6.9.7 There shall be documentation covering components that have been removed and/or disabled, and justification for components that remain enabled.

5.6.10 Remote Access

TfL must ensure that the system shall provide the capability to monitor and control all methods of access to the control system via untrusted networks.

The system owner must ensure compliance with the following minimum baseline requirements:

5.6.10.1 Systems shall only use remote access where absolutely necessary and must undergo business justification and further risk assessment to provide justification.

5.6.10.2 Remote access services shall use secure methods such as VPN and SSH.

5.6.10.3 Remote access services must route through an OT DMZ.

5.6.10.4 An OT DMZ shall be the preferred means of controlled remote access to OT systems.

5.6.10.5 Maintain the systems capability to deny access requests via untrusted networks unless approved by an assigned role.

5.6.10.6 Telnet sessions shall not be permitted.

5.6.10.7 Dial up and line modems shall not be permitted.

5.6.10.8 Maintain the systems capability to terminate a remote session either automatically after a configurable period of inactivity or manually by the user who initiated the session (Section 5.1.2 refers).

5.6.10.9 Maintain the systems multifactor authentication scheme, with an appropriate level of strength to positively identify a remote interactive user.

5.6.11 Vulnerability Management

TfL must ensure that there is the capability to manage vulnerabilities in the network and information systems to prevent disruption of TfL services.

Individual system owners must ensure that processes are implemented and maintained to comply with the principles of vulnerability management, so that the system they are responsible for can be kept secure throughout the life of the system.

The system owner must ensure compliance with the following minimum baseline requirements:

5.6.11.1 The system shall be free of known vulnerabilities on handover to operational service. Where a vulnerability cannot be resolved, suitable alternative controls must be implemented and the vulnerability, with mitigating controls and a long-term resolution plan, recorded in the project/system risk register.

5.6.11.2 The system shall not be handed over with obsolete technology in place.

5.6.11.3 Implement and maintain a process to monitor, record and analyse publicly known vulnerabilities relevant to the system to understand the risk. This will require access to documents covering the system and network configuration, high level design and asset register.

5.6.11.4 Implement and maintain a process to ensure that both publicly announced and privately notified vulnerabilities in the system are recorded and tracked. Tracked vulnerabilities must be clearly tagged with both the OT system affected and the TfL services which could be impacted if the vulnerability was exploited.

5.6.11.5 Implement and maintain a process to ensure that vulnerabilities being tracked can be assessed, prioritised, and mitigated.

5.6.11.6 Implement and maintain a process to implement a temporary mitigation solution for a vulnerability which is not exposed outside the system boundary/security Zone of the system.

5.6.11.7 Implement and maintain a process to manage and implement a temporary mitigation solution for obsolete and/or unsupported technology while pursuing migration to supported technology.

5.6.11.8 Any temporary mitigation, whether for a vulnerability or obsolete technology, must be risk assessed and recorded in the system risk register.

5.6.11.9 Maintain the systems capability to support regular tests or assessments undertaken to check for previously unknown vulnerabilities within the constituent components.

Due to the sensitive nature of OT networks and systems, operators need to carefully consider their approach to the testing of live OT, as system operation, availability and safety could be affected. Assurance could be gained without this additional risk by testing against non-operational environments or by testing individual components in a laboratory environment.

5.6.11.10 Vulnerabilities shall be rated according to the Common Vulnerability Scoring System (CVSS)

For guidance on a vulnerability management process see section 5.6.11 of G1772 Operational Technology Cyber Security Operations and Maintenance

5.6.12 Patch Management

TfL must ensure that there is the capability to deploy patches in the network and information systems to prevent disruption of TfL services.

Patches are additional pieces of code that have been developed to address specific problems or flaws in existing software. They can be part of a general service improvement plan from the manufacturer or can be in response to a specific vulnerability.

Individual system owners must ensure that processes are in place to ensure the systems they are responsible for comply with the principles of patch management and can be kept secure through life.

Applying patches to Operating System (OS) components creates another situation where significant care should be exercised in the OT environment.

The system owner must ensure compliance with the following minimum baseline requirements:

5.6.12.1 Systems will have been handed over into operation with the latest approved and validated software version and patch revision applied.

5.6.12.2 Implement and maintain a systematic and documented patch management process to monitor, record and analyse patches relevant to the system which must operate throughout the operating life of the system.

5.6.12.3 Patches must be thoroughly tested to determine they do not impact the safe operation of the system and do not introduce unexpected side effects. Regression testing is advised.

5.6.12.4 Patches must only be deployed from known secure sources i.e. from a patch management server.

5.6.12.5 Any patches which cannot be applied must be captured with the system risk register and mitigating controls identified and implemented

5.6.12.6 Patches must be risk assessed on a case by case basis and determined by the applicability to the system, the vulnerabilities that are mitigated, the priority of the vulnerability and the impact to the safety and reliability of the system.

5.6.12.7 Patches shall be applied in line with the configuration management / change management process.

5.6.12.8 Implement and maintain procedures for the test and implementation of patches.

5.6.12.9 Patches that have been risk assessed and deemed applicable for the system shall be applied at the earliest maintenance period and no later than the following:

Vulnerability Severity Rating	Remediation Period
CVSS Score 10	30 days
CVSS Score 8 or higher	90 days
CVSS Score 6 or higher	180 days
CVSS Score 4 or higher	365 days
CVSS Score 1 or higher	365 days

For guidance on a patch management process see section 5.6.12 of G1772 Operational Technology Cyber Security Operations and Maintenance

5.6.12.10 Implement and maintain procedures for the urgent testing and implementation of patches.

5.6.12.11 Patches that have been deemed urgent for the system shall be applied at the earliest maintenance period and no later than 30 days.

The need for urgent patching may be as a result of an imminent threat to the system and come several sources such as TfL's Cyber Security Team, from external agencies or TfL's partners.

5.6.13 Time Synchronisation

TfL must ensure that time is synchronised across all systems and services.

The system owner must ensure compliance with the following minimum baseline requirements:

5.6.13.1 Maintain the systems capability to synchronise with a dedicated time source through a secure interface.

5.6.13.2 Maintain the systems capability to protect the unauthorised modification of time sources.

5.7 Providing Secure Management

TfL must ensure that network and information systems that support the delivery of TfL services can be managed, operated, and maintained securely.

5.7.1 Secure Management

Systems shall be managed, operated, and maintained in a secure manner.

The system owner must ensure compliance with the following minimum baseline requirements:

5.7.1.1 Dedicated devices shall be used for the maintenance and security management of OT systems.

5.7.1.2 Devices which are used to manage and maintain systems shall be verified as free from unauthorised software and malware before being connected to conduct management or maintenance activities.

5.7.1.3 Systems shall only be administered and maintained by authorised privileged users.

5.7.1.4 Secure management processes and supporting technical information documented as part of the system development process and handed over with the system into operational service, shall be implemented and maintained.

5.7.1.5 Documents which support the system shall be stored and secured according to the criticality of the system or the impact of the loss of that system on the delivery of TfL services.

6 Detecting Cyber Security events

The following controls and considerations will contribute to detecting Cyber Security incidents within TfL's OT and establish the minimum baseline of Cyber Security measures for operating and maintaining new or upgraded systems securely. Where possible, the minimum baseline Cyber Security measures should be adopted when operating or maintaining any OT supporting TfL services, recognising that legacy systems may not have been designed with these Cyber Security controls in place.

Safety critical and service critical systems will have been risk assessed at the design stage and are expected to require additional controls above the minimum baseline, for which suggestions are shown in the notes.

6.1 Security Monitoring

TfL must ensure that systems have effective Cyber Security defences and the capability to detect Cyber Security events which affect, or have the potential to affect, the delivery of TfL services.

6.1.1 Monitoring coverage

TfL must ensure that data sources have been identified to support the timely identification of security events in the system.

The system owner must maintain the capability to meet the following minimum baseline requirements:

6.1.1.1 Security monitoring data shall be collected from identified data sources (Section 6.1.3 refers) to detect and identify security events in the system.

6.1.1.2 Maintain the systems capability to detect the presence of known indicators of compromise on the essential components of the system.

6.1.1.3 Monitoring shall be conducted of all privileged activity on the system for suspicious or undesirable activity.

6.1.1.4 There shall be monitoring in place on all network gateways and critical devices, where possible.

6.1.1.5 Maintain the network taps installed at the network choke point boundary between the OT system and any external systems.

6.1.1.6 Maintain the network taps installed at the network choke point boundary between the OT control system and its subordinate Zones.

6.1.1.7 Maintain the systems capability to collect essential information against critical services or applications (such as key servers).

6.1.1.8 Maintain the systems capability to detect the connection of unauthorised devices to the system.

6.1.1.9 There shall be documented reporting mechanisms such that any monitoring alert can allow for a timely response to events.

6.1.1.10 Maintain the centralised logging server.

6.1.1.11 Maintain the System log capability of being read locally and forwarded to the centralised logging server.

6.1.2 Securing Logs

TfL must ensure that logging data be held securely and read access to it should be granted only to accounts with a business need.

The system owner must maintain the following minimum baseline requirements:

6.1.2.1 Only authorised personnel can view logging information.

6.1.2.2 Maintain the systems restrictions to modify or delete logging data within the specified retention period, after which it can be deleted.

6.1.2.3 Maintain the systems capability to protect audit information and audit tools (if present) from unauthorised access, modification, and deletion.

6.1.2.4 Maintain the systems capability for authorised humans and/or tools to access audit logs on a read-only basis.

6.1.2.5 Maintain the systems capability to allocate sufficient audit record storage capacity according to commonly recognised recommendations for log management and system configuration.

6.1.2.6 Maintain the systems capability to provide auditing mechanisms to reduce the likelihood of such capacity being exceeded.

6.1.2.7 Maintain the systems capability to alert personnel and prevent the loss of essential services and functions in the event of an audit processing failure.

6.1.2.8 Maintain the systems capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.

> It should be noted that either overwriting the oldest audit records or halting audit log generation are possible responses to audit storage capacity being exceeded but imply the loss of potentially essential forensic information.

6.1.2.9 Implement and maintain procedures to securely extract, read and manage logging data.

Note: For safety critical and service critical systems, the following additional requirements shall apply:

6.1.2.10 Audit records on write once media.

6.1.3 Generating Alerts and Audit Records

TfL must ensure that data relating to potential security alerts is captured in the monitoring data and that alerts are triggered.

The system owner must maintain the following minimum baseline requirements:

6.1.3.1 Maintain the systems capability to generate audit records about events occurring in the system.

6.1.3.2 Audit records should be sufficient in detail to monitor the effectiveness and proper operation of the security mechanisms in place on the system.

6.1.3.3 Maintain the systems capability to generate audit records relevant to security for the following categories:

- Access control
- User activity
- Request errors
- Operating system (System, User and Security) events
- Control system events
- Use or attempts to use mobile devices
- Connection of unauthorised devices
- Backup and restore events
- Configuration changes
- Potential reconnaissance activity
- Audit log events
- Anti-malware events
- Boundary device logs
- FTP Logs
- Proxy Logs
- VPN Logs.

6.1.3.4 Maintain the systems capability to provide timestamps for use in audit record generation.

6.1.3.5 Individual audit records shall include:

- Timestamp
- Source (originating device, software process or human user account)
- Category
- Type
- Event ID
- Event result.

6.1.3.6 Alerts shall be resolved to individual assets.

6.1.3.7 Actions shall be attributed to a specific human user.

MAYOR OF LONDON
Transport for London
TfL RESTRICTED

6.1.3.8 Alerts shall be generated on suspicious activity linked to known Indicators of Compromise.

6.1.3.9 Security logs shall be reviewed regularly and, if possible, alerts should be reviewed almost continuously, in real time.

6.1.3.10 Security alerts shall be prioritised, investigated and appropriate action taken.

Note: For safety critical and service critical systems, the following additional requirements shall apply:

6.1.3.11 Internal time synchronisation.

6.1.3.12 Protection of time source integrity.

6.1.3.13 Non-repudiation for all users.

6.1.4 Identifying Security Incidents

TfL must ensure that security alerts are contextualised with knowledge of the threat and the systems, to identify those security incidents that require some form of response.

The system owner must maintain the following minimum baseline requirements:

6.1.4.1 Updates for all signature based protective technologies are received at least once every 4 weeks.

6.1.4.2 Maintain the systems capability for updates to be implemented at least every 4 weeks.

6.1.4.3 Security issues from a recognised source of threat information shall be prioritised, investigated and appropriate action taken.

6.1.4.4 Security alerts shall be prioritised, investigated and appropriate action taken.

6.1.5 Monitoring Tools and Skills

TfL must ensure that monitoring staff skills, tools, and roles, including any that are outsourced, should reflect governance and reporting requirements, expected threats and the complexities of the network or system data they protect.

The system owner must maintain the following minimum baseline requirements:

6.1.5.1 Ensure the requirements for monitoring coverage (Section 6) and incident response (Section 7) are maintained, with appropriate tools and techniques either as handed over into live service or with appropriate replacements adopted through formal change control processes.

Consideration should be given to aligning these tools and techniques with other systems for a more consistent and coordinated approach.

6.1.5.2 There shall be personnel who are responsible for the analysis, investigation and reporting of monitoring alerts covering both security and system performance.

This could involve additional personnel to create additional capacity or require existing personnel to be updated on the new system.

6.1.5.3 There shall be defined roles and skills/competence requirements to ensure that monitoring personnel, together with other personnel such as operators, system

administrators and third parties, are able to cover all parts of the monitoring and investigation process.

6.1.5.4 There shall be up to date documentation to inform monitoring personnel which TfL services are supported by the assets being monitored so that alerts or investigations can be prioritised appropriately.

6.1.5.5 There shall be up to date documented processes, procedures, and workflows for monitoring personnel to follow for the analysis, investigation and reporting of alerts.

6.1.6 Incident Reporting

TfL must ensure that the reporting requirements for Cyber Security incidents are clearly articulated and understood to ensure that the right information is provided to the right people in a timely manner to allow incidents to be resolved effectively.

The system owner must implement and maintain reporting processes and procedures and ensure that the system can generate the information required, reporting at the first available opportunity, to meet the following minimum baseline reporting requirements:

6.1.6.1 The theft or unexplained loss of cyber systems or assets, asset data which an attacker could use to improve the chances of a successful attack or circumvent installed security measures.

6.1.6.2 The unauthorised physical or electronic access to cyber systems.

6.1.6.3 The compromise of a Cyber Assurance of Physical Security Systems (CAPSS) verified system protecting a Railway Asset.

6.1.6.4 The occurrence of successful or suspected attempted jamming of radio communication systems such as (but not limited to) mobile phones, portable credit/debit card payment systems, radios, Global Positioning System (GPS) radio navigation systems or Global System for Mobile Communications-Railway (GSM-R).

6.1.6.5 The unauthorised addition or modification of software or data on cyber systems.

6.1.6.6 The unauthorised destruction or disruption of software or data.

6.1.6.7 The malware infection of assets or attempted cyber intrusion.

6.1.6.8 The unauthorised physical access to secure rooms.

6.1.6.9 All incident reports must be made to the TfL Security Operations Centre at the earliest opportunity.

6.1.6.10 All incident reports relating to NIS systems must be made within 72 hours to the competent authority.

6.1.6.11 All Cyber Security Incidents must be accurately recorded and reported using the standard procedure and a consistent approach. This must include, but is not limited to:

a) Time and date of the Incident

b) Reference

c) Title

d) Point of contact/who reported the Incident

e) Brief description of the Incident

f) What systems and locations are affected

g) Updated comments

h) Actions taken and resolution notes

i) Resolution categories

j) All required information to ensure that all relevant data is captured to prevent this in future or to ensure that we are prepared next time.

6.1.6.12 All activities involved in a Cyber Security Incident shall be logged for later analysis.

6.1.6.13 All Cyber Security Incidents must be logged by Incident type (service) and symptom (service component) in order to ensure Incidents are correctly handled.

6.1.6.14 All Cyber Security Incidents must have clear set severity, impact and criticality levels to ensure they are dealt with appropriately.

SEV5	Critical Incident. Critical compromise, public affected. Multiple systems/devices affected or data breach. Major disruption or publicly displayed attack.
SEV4	Major Incident. Severe impact or compromise. Severe compromise, public affected. Multiple TfL devices/users affected or data breach. Major disruption or publicly displayed attack
SEV3	High Incident High impact or compromise. Multiple TfL devices/users affected. TfL users unable to work with job-dependant services
SEV2	Medium Incident Intermittent Incidents or Security Alerts, but not critical.
SEV1	Low Information or false positive. No security impact.

6.1.6.15 System owners and subject matter experts must support and co-operate with Cyber Security to ensure correct identification and response to Cyber Security Incidents.

6.1.6.16 Digital evidence must be preserved where possible during collection, storage and examination to help with Cyber Security Incident investigations.

7 Minimising the impact of Cyber Security incidents

The following controls will contribute to minimising the impact of a Cyber Security incident on TfL's OT and establish the minimum baseline of Cyber Security measures for operating and maintaining new or upgraded systems securely. Where possible, the minimum baseline Cyber Security measures should be adopted when operating or maintaining any OT supporting TfL services, recognising that legacy systems may not have been designed with these Cyber Security controls in place.

Safety critical and service critical systems will have been risk assessed at the design stage and are expected to require additional controls above the minimum baseline, for which suggestions are shown in the notes.

7.1 Incident response and recovery planning

TfL must be prepared to restore TfL services following disruption as a result of a cyber incident and must ensure that there are well-defined and tested incident management processes in place, that aim to ensure continuity of essential functions in the event of system or service failure.

Mitigation activities designed to contain or limit the impact of compromise are also in place.

An incident response plan is the documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of incidents against an organisation's information systems. Response should be measured first and foremost against the "service being provided," not just the system that was compromised.

7.1.1 Business Continuity Plan

TfL must ensure that new systems and upgrades are included in the Business Continuity Plan, which will identify procedures for maintaining and/or re-establishing essential business operations while recovering from a significant disruption.

The system owner must maintain the following minimum baseline requirements:

7.1.1.1 Recovery objectives shall be documented for the systems involved, based on business needs and reviewed annually.

7.1.1.2 The impact to TfL services because of significant disruption or system loss shall be documented and reviewed annually.

7.1.1.3 Continuity plans shall be maintained, at least annually, to ensure that business processes can be restored in accordance with recovery objectives.

7.1.1.4 The business continuity plan shall be updated, at least annually, to include any learning from experience (either exercise or real) or system/process changes.

7.1.1.5 Implement and maintain backup and restore procedures that support the business continuity plan.

7.1.2 Response and Recovery Plan

TfL must ensure that cyber incident response plans are updated with new and updated systems.

The system owner must maintain the following minimum baseline requirements:

7.1.2.1 Implement and maintain the overall cyber elements of an incident response plan or dedicated cyber incident response plan that identifies responsible personnel and defines actions to be performed by designated individuals shall be updated whenever personnel or roles change. The plan must document the actions to be taken in the event of a Cyber Security incident and those listed in Section 6.1.6.

7.1.2.2 The various types of OT incidents should be identified and classified as to potential impact so that a proper response can be formulated for each potential incident.

7.1.2.3 The systems and supporting technologies required to restore operations are known, documented and in line with TfL business continuity, disaster recovery and risk management processes.

7.1.2.4 The incident response plan shall be communicated to all appropriate organisations.

7.1.2.5 The response plan shall be tested at regular intervals, at least annually, to ensure the plan remains fit for purpose and that personnel involved understand their roles.

7.1.2.6 Implement and maintain procedures to support the activities as determined by the cyber elements of an incident response plan or dedicated cyber incident response plan. The procedures must document the actions to be taken in the event of a Cyber Security incident and those listed in Section 6.1.6.

7.1.2.7 Maintain offline and hardcopies of incident response plans and procedures.

7.1.3 System recovery

TfL must ensure that the system provides the capability to recover and reconstitute to a known secure state after a disruption or failure.

System recovery and reconstitution to a known secure state means that all system parameters (either default or configurable) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are re-established, system documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded and the system is fully tested and functional.

The system owner must maintain the following minimum baseline requirements:

7.1.3.1 The sequence in which systems, networks and supporting technologies are recovered to restore the systems supporting the delivery of TfL services shall be known, documented, and updated to reflect system changes through life.

7.1.3.2 The interdependencies between the systems and the supporting technologies shall be understood, documented, and updated to reflect system changes through life.

7.1.3.3 The capability to switch to and from an emergency power supply without affecting the existing security state or enter a documented degraded mode.

7.1.3.4 There may be instances where compensating countermeasures such as physical door access control may be affected by loss of base power supply, in which case the emergency power supply should cover those associated systems. If this is not possible, other compensating countermeasures may be needed during such an emergency situation.

7.2 Backups

TfL must ensure that there are accessible and secured current backups of data and information needed to recover network and information systems which support the TfL services.

TfL must ensure that there are backups of all systems, software, licenses, configurations, data, and other relevant information required to enable recovery of individual devices or entire networks and systems supporting the delivery of TfL services.

The system owner must maintain the following minimum baseline requirements for backups from Section 5.5.7.

7.3 Incident lessons learned

TfL must ensure that following an incident or exercise, a root cause analysis shall be conducted to identify measures to prevent reoccurrence based upon incident or exercise.

7.3.1 Lessons Learned

TfL must ensure that lessons are learned from any incident or exercise and that documentation and processes are updated to reflect those lessons.

The system owner must meet the following minimum baseline requirements:

7.3.1.1 The details of an identified incident shall be documented to record the incident, the response and the lessons learned.

7.3.1.2 Exercise scenarios should be undertaken to ensure that different aspects of the response plan are tested on a periodic, at least annual, basis and to ensure that the collective response team gain benefit from each successive exercise. Exercises must be considered as learning opportunities and lessons identified during exercise scenarios must be fed back into the response process.

7.3.1.3 System documentation and incident response processes shall be reviewed and updated following an incident or exercise.

8 Supporting Information

8.1 Background

Cyber Security should be considered as an integral part of any review for any OT and where possible should be integrated into existing safety, environmental, operational or risk considerations. This should reflect that cyber could be a potential cause of a failure and needs to be captured as part of the response or recovery process, rather than a separate consideration.

8.2 Customer Considerations

Whilst Cyber Security for OT should not be at the forefront of customer considerations, it should form part of the wider safe, secure and reliable message.

9 Guidance

For further advice and guidance in support of this standard, contact the Cyber Security team CyberSecurityGRC@tfl.gov.uk

10 Person accountable for this document

Name	Job title
Paul Richardson	Cyber Security Assurance Manager

11 Definitions

Term	Definition	Source
Operational Technology	A collection of personnel, processes, hardware and software that can affect or influence the safe, secure and reliable operation of a physical process or asset.	Jargon Buster
Conduit	Security groupings for the communications of information into, out of and within the security Zones/networks	Jargon Buster
Cyber Security	Cyber Security is the use of people, process and technology controls to protect electronic devices, networks, software and data from unauthorised access or attacks, to ensure the usability, reliability, confidentiality, integrity, resilience and safety of the network.	Jargon Buster
Internet	This public data network is considered hostile in the context of the ICS.	Jargon Buster
Protection Systems	Protection Systems, Safety-Instrumented System and Emergency Shutdown Systems.	Jargon Buster
Zones	A grouping of electronic assets that share common Cyber Security requirements.	Jargon Buster

12 Abbreviations

Abbreviation	Meaning
CCTV	Closed Circuit Television
CPNI	Centre for the Protection of National Infrastructure
CSPRNG	Cryptographically Secure Pseudorandom Number Generators
DMZ	De-Militarised Zone
FAT	Factory Acceptance Testing
HMI	Human Machine Interface
HR	Human Resources

Abbreviation	Meaning
ICS	Industrial Control Systems
IT	Information Technology
LAN	Local Area Network
MFA	Multi Factor Authentication
OS	Operating System
OT	Operational Technology
PLC	Programmable Logic Controllers
RTU	Remote Terminal Units
SCADA	Supervisory Control and Data Acquisition
SIS	Safety-Instrumented System
SMS	Short Messaging System
SPA	Single Point of Accountability
VLAN	Virtual Local Area Network
VPN	Virtual Private Network

13 References

Document no.	Title or URL
R1770	Operational Technology Cyber Security - Framework
S1771	Operational Technology Cyber Security – Projects and Upgrades
S1782	Information Security Classification
S1147	Surveillance and Security Systems
S1747	Physical Security of IT Equipment
G1772	Operational Technology Cyber Security – Operations and Maintenance
G1134	Personnel Security – Insider Threats
Network Security	https://transportforlondon.sharepoint.com/sites/TMSManagementSystem/Management%20System/Forms/NetworkSecurityMS.aspx
N/A	NIS CAF
HSE OG86v2	Cyber Security for Industrial Automation and Control Systems (IACS) Edition 2
IEC 62443-2-1	Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program
IEC 62443-3-3	Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels
N/A	CPNI Good Practice Guide – Process Control and SCADA Security
NIST SP800-82	Guide to Industrial Control System (ICS) Security
EN50128	Railway applications - Communication, signalling and processing systems - Software for railway control and Protection Systems

MAYOR OF LONDON
Transport for London
TfL RESTRICTED

Document no.	Title or URL
EN50129	Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling
EN50519	Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems

14 Document history

Issue no.	Date	Changes	Author
A1	December 2021	New standard published in accordance with Change Request CR-15204.	Tim Parker

MAYOR OF LONDON
Transport for London
TfL RESTRICTED

Transport for London

Invitation to Quote

Electric Vehicle Infrastructure Delivery (EVID)
Tranche 2, Batch 1

Volume 2

Appendix K_3

Cryptography

COMMERCIAL IN CONFIDENCE

TfL Restricted

Standard

S1740 A3 Cryptography

Contents

1 Purpose 2
2 Scope 2
3 Requirements 2
3.1 Cryptography Controls 2
3.2 Data encryption 2
3.3 Key generation and management 3
3.4 Certificate management 4
3.5 Virtual Private Network (VPN) connections 4
3.6 SSH (Secure Shell) 4
3.7 IPsec 5
3.8 SSL/TLS 5
3.9 Email security 6
4 Responsibilities 6
4.1 All IT / Security Resource 6
5 Supporting information 6
6 Person accountable for this document 6
7 Definitions 6
8 Abbreviations 8
9 References 8
10 Document history 8

MAYOR OF LONDON
Transport for London
TfL RESTRICTED

1 Purpose

This standard detail the requirements for the management of TfL cryptography considerations utilising the associated information security controls which are within scope of TfL's IT Information Security Management System (ISMS).

This standard ensures alignment to the Information Security Standard (ISO27001), the TfL Management System (TMS) and TfL's Information Technology Security Policy (P116) which, combined with the ISMS, systematically manages and protects the confidentiality, integrity and availability of TfL's information assets from threats and vulnerabilities.

2 Scope

The standard applies to all Information Technology (IT), cyber security and technical employees who have responsibilities for cryptography protocols, implementation of security certificates and accountability for TfL infrastructure.

This standard must be followed at all times and updated as industry cryptography protocols are introduced.

3 Requirements

The standard covers how employees, defined within the above Scope, should be implementing cryptography protocols securing TfL servers, applications, and communication interfaces.

3.1 Cryptography Controls

Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

3.2 Data encryption

- All data classified as TFL RESTRICTED or above must be encrypted in transit and at rest.
- Only the following encryption standards, authorised by the Cyber Security Team, must be used:
    - Symmetric/Block Encryption – Advanced Encryption Standard (AES)-256
    - Asymmetric Encryption – RSA 2048/3072/4096.
- Symmetric Encryption must use AES-256 in Cipher Block Chaining (CBC) or Cipher Feedback (CFB) mode or XTS mode with a unique Data Encryption Key (DEK) and IV. Note: ECB mode must not be used.
- The mechanisms for how these standards are achieved either through software encryption, e.g., BitLocker or hardware encryption, e.g., Hardware Security Modules (HSMs) must be determined based upon the level of risk and agreed with the Cyber Security team.

3.3 Key generation and management

- All encryption keys (except for public keys) must be:
  - Changed from any default values
  - Unique to each instance in which they are used
  - Generated by a Cyber Security authorised Cryptographically Secure Pseudorandom Number Generator (CSPNG) and not specified by a user
  - 128bits for non-elliptic curve generated keys
  - 256bits for elliptic curve generated keys
  - Encrypted in transit using AES-256 encryption in Counter (CTR) mode, with CBC-MAC (CCM) or Galois/Counter Mode (GCM).
- As part of authentication all keys and passphrases must be:
  - Hashed using at least one round of Secure Hash Algorithm (SHA)-256
  - Uniquely salted with salts of at least 32 bytes (64 bytes if supported).
- Keys and passwords must be stored securely whether in a Cyber Security authorised key vault or locally in a hashed format, which:
  - Ensures unique salts of at least 32 bytes (64 bytes if supported) for each key and password are used
  - Uses either PDFKD2-HMAC-SHA256 or SCRYPT (using specific set key derivation function) hashing
  - Utilises AES-256 encryption in CCM or GCM mode
  - Enforces Cyber Security approved methods of multi-factor authentication
  - Segregate the key vault from systems for which it holds the keys/certificates.
- System owners are responsible for ensuring key renewal/refresh is carried out in line with Cyber Security authorised timescales.
- Access to encryption keys must:
  - Only be granted to those who require access for their role and be treated as privileged access in line with the System access control standard.
  - Be subject to strict security logging, monitoring and audit in line with the corresponding standard.

3.4 Certificate management

- X.509v3 security certificates must use the appropriate cryptographic profiles (BASELINE / ENHANCED) within this standard, depending on the level of risk as agreed with the Cyber Security team.
- Certificates must be generated by a privileged user for the device being used.
- Private keys for certificates must stay upon the device on which they are being used operationally.
- End entity certificates must only be valid for 1 year, or the expected life of the device, whichever is the shorter timeframe of the two.
- Certificates for single or low numbers of links may have the relevant public keys for other Virtual Private Network (VPN) connected devices preinstalled to reduce overheads.
- Root and sub-CA(s) must have pre-set expiration dates of:
    - The anticipated end of life of the network; OR
    - Sub CA = 31st Dec 2022 AND Root CA = 31st Dec 2030.
- Wildcard certificates must only be used with Cyber Security team authorisation and the business justification must be recorded.

3.5 Virtual Private Network (VPN) connections

- Network connections which require protection/security must utilise either Internet Protocol Security (IPsec), Secure Sockets Layer (SSL) / Transport Layer Security (TLS) or Secure Shell (SSH), depending on the user case and Cyber Security assessment. This may be deployed as:
    - A software client running on an End User Device (EUD)
    - A dedicated hardware appliance such as a VPN gateway
    - Enhanced functionality on networking infrastructure equipment such as routers
- All VPNs must be end-to-end, i.e., end user device to server/target.

3.6 SSH (Secure Shell)

- All SSH access must follow the System access control standard
- All instances of IPsec must use one of the following cipher suite profiles (depending upon risk assessment):
    - BASELINE profile (all categories with higher recommended options must also be supported):

Algorithm Type	Description
Version	SSH-2
Cipher	AES-128 in CTR mode
MACs	HMAC-SHA2-256
Key Exchange (kex)	DH Group Sha-256

- ENHANCED (all categories with higher recommended options must also be supported):

Algorithm Type	Description
Version	SSH-2
Cipher	AES-256 in GCM mode
MACs	HMAC-SHA2-256-etm
Key Exchange (kex)	Curve25519-Sha256

3.7 IPsec

- All instances of IPsec must use one of the following cipher suite profiles (depending on the results of a risk assessment):
  - BASELINE profile (RFC compliant):

IKEv1	Requirement
Version	AES-128 in CBC mode
Pseudo-random function	HMAC-SHA256
Diffie-Hellman Group	Group 14 (2048-bit MODP Group)
Authentication	RSA signatures (2048 bits) and SHA-256

  - ENHANCED profile

IKEv1	Requirement
Version	AES-256 in GCM mode
Pseudo-random function	HMAC-SHA256
Diffie-Hellman Group	256bit random ECP
Authentication	ECDSA-256 with SHA256 on Prime-256 curve

3.8 SSL/TLS

- Only supported TLS versions (as detailed below) must be used. The use of any SSL versions is not authorised by the Cyber Security team
- Web servers must:
  - Implement TLS over HTTP (HTTPS) in all instances
  - Automatically redirect all users to HTTPS version
  - Enable HTTP Strict Transport Security (HSTS)
- Implementation of TLS must conform to one of two Cyber Security authorised cryptographic profiles, depending on the results of a risk assessment.
  - BASELINE profile (all categories with higher recommended options must also be supported):

Algorithm Type	Description
Version	TLS 1.2
Cipher Suite	TLS_ECDHE_RSA_AES_128_CBC_SHA256
Encryption	AES-128 in CBC mode
Authentication	X.509v3 certificates with RSA signatures (2048 bits)
Key Exchange (kex)	ECDH using P-256 curve
MAC	HMAC-SHA-256
Certificate Signature	Sha256withRSAEncryption

- ENHANCED profile (all categories with higher recommended options must also be supported):

Algorithm Type	Description
Version	TLS v1.3
Cipher Suite	TLS_ECDHE_ECDSA_AES_256_GCM_SHA384
Encryption	AES-256 in GCM mode
Authentication	ECDSA
Key Exchange (kex)	ECDH using P-256 curve
MAC	AHEAD
Certificate Signature	Ecdsa-with-SHA256

3.9 Email security

- Domain-based Message Authentication, Reporting and Conformance (DMARC) must be set up and appropriately configured to ensure:
  - Recipients are notified that there is a DMARC policy
  - Messages that fail DMARC are treated as spam.

4 Responsibilities

4.1 All IT / Security Resource

Controls stipulated within this standard are defined and owned by the TfL Cyber Security Team and are implemented by IT / infrastructure resource ensuring the standard is adhered to at all times.

5 Supporting information

Advice and guidance about this standard can be obtained from the Cyber Security team by emailing cybersec@tfl.gov.uk.

6 Person accountable for this document

Name	Job title
Paul Richardson	Cyber Security Assurance Manager

7 Definitions

Term	Definition	Source
ISO/IEC 27001	ISO standard for Information Security	Jargon Buster

Term	Definition	Source
Advance Encryption Standard	A symmetric cryptographic algorithm used for encrypting/ decrypting data.	Jargon Buster
Cipher Block Chaining (CBC)	An encryption mode used for encrypting/decrypting data.	Jargon Buster
Counter with CBC-MAC (CCM)	Combines CBC-MAC with the Counter (CTR) mode on encryption.	Jargon Buster
Cipher Feedback (CFB)	An encryption mode used for encrypting/decrypting data (closely associated to CBC).	Jargon Buster
Counter (CTR)	An encryption mode which turns block ciphers into stream ciphers.	Jargon Buster
Data Encryption Key (DEK)	Most commonly used by Microsoft based systems.	Jargon Buster
Domain Message Authentication Reporting and Conformance (DMARC)	A system used for validating emails, their origins and preventing email spoofing and phishing.	Jargon Buster
Elliptic Curve Digital Signature Algorithm (ECDSA)	A digital signature algorithm.	Jargon Buster
Galois/Counter Mode (GCM)	An encryption mode used for encrypting/decrypting data and data integrity checking.	Jargon Buster
Keyed-Hash Message Authentication Code (HMAC)	A specific message authentication code (MAC) which combines with a hash function and secret key.	Jargon Buster
Hypertext Transfer Protocol (Secure) (HTTP(S))	A protocol used for (secure) communication over a network i.e., the Internet.	Jargon Buster
Request for Comments (RFC)	An Internet Engineering Task Force (IETF) and Internet Society (ISOC) standard.	Jargon Buster
Secure Hash Algorithm (SHA)	A special class of hash functions which takes a variable input of data and outputs a deterministic string of characters dependent on a number of variables.	Jargon Buster
Secure Sockets Layer (SSL)	A cryptographic protocol designed to provide security for digital communications which is no longer supported	Jargon Buster
Transport Layer Security (TLS)	Transport Layer Security – an updated version of SSL with later version (1.2 & 1.3) providing supported secure communications and data integrity.	Jargon Buster

8 Abbreviations

Abbreviation	Meaning
AES	Advance Encryption Standard
CBC	Cipher Block Chaining
CCM	Counter with CBC-MAC
CFB	Cipher Feedback
CSPNG	Cryptographically Secure Pseudorandom Number Generator
CTR	Counter
DEK	Data Encryption Key
DMARC	Domain Message Authentication Reporting and Conformance
ECDSA	Elliptic Curve Digital Signature Algorithm
EUD	End User Device
GCM	Galois/Counter Mode
HMAC	Keyed-Hash Message Authentication Code
HTTP(S)	Hypertext Transfer Protocol (Secure)
IPsec	Internet Protocol Security
RFC	Request for Comments
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TfL	Transport for London
TLS	Transport Layer Security
VPN	Virtual Private Network

9 References

Document no.	Title or URL
P116	Information Technology Security Policy

10 Document history

Issue no	Date	Changes	Author
A1	July 2017	New standard produced as per change No. 04917.	Paul Beverley
A2	March 2018	Changes made following annual review as per Change No. CR-10280.	Haider Sarwar
A3	March 2022	Significant edit to align with ISO27001 as per Change No. CR-15515.	Alison Beckwith

MAYOR OF LONDON
Transport for London
TfL RESTRICTED

Transport for London

Invitation to Quote

Electric Vehicle Infrastructure Delivery (EVID)
Tranche 2, Batch 1

Volume 2

Appendix K_4

CSM Schedule Payments

COMMERCIAL IN CONFIDENCE

TfL Restricted

Cyber Security Management Schedule
Payments
Version 1.0



TfL RESTRICTED

Document Information

Document name:	Cyber Security Management Schedule – Payments
Brief description:	This Schedule defines the cyber security requirements for TfL Suppliers who deliver PCI DSS managed environments
Document Author:	Roger Dias
Date of Issue:	Version 1.0
Next review date:	13-02-2023

Document history

Version No.	Issue Date.	Changed by.	Changes.
1.0	13-02-2023	Roger Dias	Document Published by CISSG

Circulation List

Department / Division:	Name:	Date:
Pan-TfL	Pan-TfL	13-02-2023wa

Contents

1. Security Standards 4
2. Security Principles 5
3. Security Management Plan 6
ANNEX 1 – Security Requirements 7
ANNEX 2 – Definitions 17
ANNEX 3 – List of relevant Policies and Standards 21

1. Security Standards

1.1. This Schedule uses the definitions set out on ANNEX 2.

1.2. Where the Supplier is processing or storing TfL Data on a regular basis, there will be a requirement for the Supplier to be:

1.2.1. Independently certified to ISO/IEC 27001:2013 or latest version, with a scope which covers TfL's Data.

1.2.1.1. Independently tested to verify that the systems used to process TfL Data meet the requirements of the UK government promoted Cyber Essentials Scheme and/or Network & Information Systems (NIS) Directive.

1.3. Where the Supplier is transmitting, storing and/or processing Payment Card Data, the Supplier must ensure that they comply with all card scheme rules and regulations, including but not limited to the most recent version of the Payment Card Industry Data Security Standard ("PCI DSS") as promulgated by the Payment Card Standards Security Council ("PCI SSC") as updated from time to time and as they apply to the Services. TfL require proof of such compliance by an externally signed Attestation of Compliance (AoC) and a Report on Compliance (RoC) at which time the Supplier shall provide that proof within 3 months. The Supplier shall perform regular reviews of their security, availability and processing integrity, reporting to TfL any identified vulnerability per PCI DSS requirements.

1.3.1. The Supplier agrees and acknowledges that they are responsible for the security of Cardholder Data and the Supplier shall indemnify TfL from and against all penalties, costs and expenses which may be suffered, paid or incurred by TfL as a consequence of the Supplier's failure to comply with the PCI DSS requirements.

1.3.2. The Supplier shall limit storage amount and retention time of card holder data to that which is required for business, legal, and/or regulatory purposes, as required by TfL's Data Retention Policy as issued from time to time.

1.3.3. The Supplier shall perform a PCI compliance assessment for all work relating to TfL and perform any remedial action required within a timescale agreed with TfL

2. Security Principles

2.1. The Supplier acknowledges that security, data protection and confidentiality are of fundamental importance in relation to its performance of this Agreement and TfL's ability to retain public confidence. The Supplier shall always comply with the security principles set out in this paragraph in the performance of this Agreement.

2.2. In recognition of the importance that TfL places on security, data protection and confidentiality, the Supplier shall ensure that a director or relevant individual of the Service Provider, as agreed by TfL, is made aware of the risks set out in the Security Management Plan and is assigned overall responsibility for ensuring that:

2.2.1. appropriate members of the Supplier Personnel and the Supplier's management team take responsibility for managing the different levels of security risk and promoting a risk management culture.

2.2.2. a Security Risk Register is produced and maintained throughout the Term and that all Security Risks are documented in an appropriate manner and are included in any contract risk register for this Agreement if one is in place. The Security Risk Register must be available for audit when reasonably required by TfL.

2.2.3. a Service Asset Register is produced and maintained throughout the Term and that all Service Assets are documented in an appropriate manner in the service asset register and shall identify the criticality of the relevant supplier assets in the delivery of this Agreement. The Service Providers service asset register must be available for audit when reasonably required by TfL.

2.2.4. supporting policies are implemented (where relevant) and communicated with Supplier Personnel.

2.3. The Supplier shall, and its sub-contractors shall, at all times ensure that:

2.3.1. security threats to TfL Data, the Supplier's IT environment, and the Services are minimised and mitigated.

2.3.2. the Services fully comply at all times with:

2.3.2.1. the Security Requirements set out in Annex 1 and 3 of this Schedule, or otherwise agreed in the Security Management Plan

2.3.2.2. the Security Management Plan.

2.3.2.3. Good Industry Practice.

2.4. The Supplier shall not (and shall ensure that the sub-contractors shall not) use any Cloud Services for, or in connection with, the performance of this Agreement (including in relation to any TfL Data) without TfL's prior written approval and, if so provided, the Supplier shall ensure that any such Cloud Services complies with this Schedule.

3. Security Management Plan

3.1. Within the timescales identified in ANNEX 1 (Security Reporting) the Supplier shall submit to TfL for Approval (and thereafter maintain) a Security Management Plan which as a minimum shall:

3.1.1. set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Services and all processes associated with the delivery of the Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure the Services comply with this Schedule.

3.1.2. state any other cyber security industry standards over and above those set out in this Schedule which are applicable to the Services.

3.1.3. state all applicable Law which relates to the security of the Services; and

3.1.4. state how the Supplier shall comply with any other security requirements TfL may

3.1.5. reasonably request from time to time.

3.2. The Supplier shall review and update the Security Management Plan at least annually and as required in response to:

3.2.1. changes to the Cyber Security Standards

3.2.2. emerging changes in Good Industry Practice

3.2.3. any relevant Contract Change and/or associated processes

3.2.4. any new perceived or changed security threats and

3.2.5. any reasonable request by TfL.

3.3. The Supplier shall submit any amendments to the Security Management Plan for Approval by TfL.

ANNEX 1 – Security Requirements

1. Risk Management

1.1. The Supplier shall:

1.1.1. implement a Risk Management process for the purpose of identifying, assessing, mitigating, monitoring, and reporting upon cyber security risks.

1.1.2. organise and manage a risk management forum where risks identified will be discussed and addressed (*Security Reporting- Security Risks within the Risk Register*).

1.1.3. conduct threat and risk assessments on any part of the Services that are new or have been materially changed since the last threat and risk assessment was conducted (*Security Reporting- Security Risk Treatment Plan*).

1.1.4. risks identified will be discussed with the relevant member of TfL.

2. Engagement and Training

2.1. The Supplier shall:

2.1.1. screen all Service Provider Personnel prior to the Supplier authorizing access to the Services the Supplier is performing on TfL's behalf. *(Security Reporting - Joiners, Movers & Leavers Notification)*

2.1.2. conduct criminal record checks on all Supplier Personnel who have access to any Services the Supplier operating on behalf of or TfL. The level of checks should be consistent with British Standard 7858 (BS7858- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/417085/BS7858.pdf

2.1.3. ensure all Supplier Personnel have been vetted in accordance with HMG Guidance for overseas individuals – https://www.gov.uk/government/publications/criminal-records-checks-for-overseas-applicants

2.1.4. make a reasonable determination of whether the individual constitutes an unreasonable security risk taking into consideration the duties of the

individual, the type and sensitivity of information to which the individual may be exposed, and all applicable laws.

2.1.5. require all Supplier Personnel to proactively disclose criminal offences to the Supplier unless prohibited by applicable law.

2.1.6. ensure that all persons employed or retained to perform the Services receive security awareness training annually and supervision at a level and in substance that is appropriate to that individual's position and the Supplier's obligations under this Agreement.

2.1.7. not permit any person the Supplier hires or uses to access or obtain any TfL Data unless that person is contractually bound to the Supplier in writing to keep TfL Data confidential on terms no less protective than the terms applicable to the Supplier under this Agreement.

3. Asset Management

3.1. The Supplier shall implement controls to manage Service Assets throughout its lifecycle. These controls will include processes for acquiring, using, maintaining, and disposing Service Assets.

3.2. Service Assets used to access or manage TfL Data and Services must be under the authority of the Supplier or TfL and have a standard set of security controls deployed upon them. These Assets must be placed into a 'known good' state prior to being provisioned into the environment of the Supplier. Unless otherwise agreed with the TfL in writing, all Supplier assets are expected to meet the set of security requirements set out within PCI DSS requirements https://www.pcisecuritystandards.org/

3.3. The Supplier shall:

3.3.1. maintain an inventory of all Service Assets.

3.3.2. use secure methods when disposing of Service Assets.

3.3.3. maintain records of the disposal of Service Assets.

3.3.4. through the operation of the Supplier's Change Management process, manage changes to any Service Asset.

4. Architecture and Configuration

4.1. The Supplier shall implement and maintain security assets such as industry standard firewalls that protect the perimeter and internal components of the Services environment.

4.2. The Supplier shall follow industry standards for Asset Hardening and Secure Configuration.

4.3. The Supplier shall remove or disable unnecessary utilities from operating systems, configurations and restrict access rights to least privilege.

4.4. The Supplier will ensure that any preconfigured passwords delivered with any Service Assets are changed prior to their implementation for use in the Services environment.

4.5. Where the Supplier manages user authentication controls for the Service Provider Personnel to access the Services, the Supplier must:

4.5.1. enforce minimum password complexity, such as requiring passwords to be case sensitive, or requiring passwords to contain a minimum of twelve characters and a combination of upper-case letters, lower-case letters, numbers, and/or special characters.

4.5.2. require regular change of passwords at predetermined intervals, and which limit reuse.

4.5.3. require multi-factor authentication for privileged access.

4.6. The Supplier will establish a software development lifecycle for the purpose of defining, acquiring, developing, enhancing, modifying, testing, or implementing information systems.

4.7. The Supplier shall ensure that web-based and mobile applications used to store, receive, send, control or access TfL Data are monitored, controlled and secure.

4.8. The Supplier shall implement and manage a Change Management process to manage changes that occur within the Services environment.

5. Vulnerability Management

5.1. The Supplier will implement and maintain a Vulnerability Management programme, which will include the following elements:

5.2. security patches will be applied to Service Assets as soon as possible in line with vendor recommendations in accordance with the Change Management Process.

5.3. a process to test rogue wireless access points. (*Security Reporting - Wireless Access Point Scan Reports)*

5.4. Internal and external network vulnerability tests that are carried out at least quarterly. An external, qualified party should be resourced to carry out the external network vulnerability tests. *(Security Reporting - Penetration Test Report)*

5.5. External and internal penetration tests using the Supplier's penetration testing methodology that is based on industry-accepted penetration testing approaches that cover the all-relevant systems and include application-layer as well as network-layer tests. All test results are kept on record and any findings are remediated in a timely manner.

5.5.1. The Supplier will ensure that all penetration tests conducted upon the Services it provides are performed by approximately industry accredited organisations.

5.6. The Supplier shall implement an Intrusion Detection System (IDS) and/or an Intrusion Prevention Solution (IPS) technique to detect / prevent and alert on intrusions into the network.

5.7. The Supplier shall maintain industry standard processes for defending against malware / Trojans / virus infections. The Supplier shall maintain a programme of anti-malware/anti-virus updates to keep provisioned Assets free of infection.

6. Supply Chain Security

6.1. The Supplier must maintain an inventory of all suppliers / sub-contractors it utilises. This should be in the form of a supplier matrix with roles and responsibilities defined.

6.2. The Supplier must ensure that its suppliers and sub-contractors involved in the provision of Services meet or exceed the standards set forth in this Schedule.

6.3. The Supplier must conduct security assessments upon its supply chain to ensure all suppliers of Services to its present a low or no risk to the Service it is providing to TfL.

7. Incident Management

7.1. The Supplier will implement and maintain an Incident Management Plan which will be used to respond on breaches to the Service. The Incident Management Plan will include the following:

7.1.1. Definition of roles, responsibilities, and communication and contact strategies in the event of a compromise, including notification of customers.

7.1.2. Specific incident response procedures.

7.1.3. Analysis of legal requirements for reporting compromises.

7.1.4. Coverage of all critical system components.

7.1.5. Regular review and testing of the Incident Management Plan.

7.1.6. Incident management Support Personnel that are available to support the Services.

7.1.7. Training of Supplier Personnel.

7.1.8. Inclusion of alerts from all security monitoring systems.

7.1.9. Modification and evolution of the Incident Management Plan according to lessons learned and to incorporate industry developments.

8. Logging and Monitoring

8.1. The Supplier shall implement and maintain a solution which enables all access to network resources and Data to be tracked and monitored using a centralized logging mechanism that allows thorough tracking, alerting, and analysis on a regular basis (at least daily) as well as when an abnormality/incident occurs.

8.2. The Supplier shall deploy and maintain a File-Integrity Monitoring solution to alert Supplier Personnel via its centralized solution to unauthorized modification of critical systems.

8.3. The Supplier shall ensure that all systems shall be provided with correct and consistent time and audit trails that are secure and protected, including File-Integrity Monitoring for Data classified as Confidential to prevent changes of existing Log Files and/or generate system alerts.

8.4. The Supplier shall ensure that audit trails for critical systems are kept for a period in-line with industry standards.

9. Data Security

9.1. The Supplier shall:

9.1.1. implement and maintain a Key Management Solution in-line with industry standards.

9.1.2. implement and maintain encryption of TfL Data while it is at rest.

9.1.3. implement and maintain encryption of TfL Data while it is in transit.

9.1.4. not provide encryption keys used to secure TfL Data to a third party or the ability to break such encryption.

9.1.5. implement and maintain the logical separation of TFL Data, even in the case of equipment or technology failure.

9.1.6. implement, where supported by available technology, the logical separation of audit records related to TfL Data and activities, even in the case of equipment or technology failure, segregate tenancy traffic from management network traffic.

9.1.7. not use TfL Data for test or development purposes without the written approval of TfL.

9.2. The Supplier shall segment the environment to ensure specific classified types of Data are not accessible to unauthorized individuals.

9.3. The Supplier shall ensure that all Service Assets have appropriate tools or applications installed to protect against malicious software.

10. Identity and Access Management

10.1. Where the Supplier's Personnel are accessing any part of the Supplier's Systems that may contain TfL Data, the Supplier must:

10.1.1. implement access control policies and procedures that address onboarding, off-boarding, transition between roles, regular access reviews, limitations and usage control of administrator privileges, and inactivity timeouts.

10.1.2. identify and segregate conflicting duties and areas of responsibility, such as separation of duties.

10.1.3. maintain a current and accurate inventory of computer accounts.

10.1.4. review the inventory of computer accounts on a regular basis to identify dormant, fictitious, or unused accounts.

10.1.5. enforce principles of “least privilege” and “need to know”.

10.1.6. review user access rights on a regular basis to identify excessive privileges.

10.1.7. enforce a limit of logon attempts and concurrent sessions.

10.1.8. ensure that all users of the Services are allocated a single unique ID for accessing the Services environment.

10.1.9. ensure any system administration functionality is strictly controlled and restricted to those Supplier Personnel who need to have access to such functionality and that the ability of Supplier Personnel to change the configuration of the Service Assets is appropriately limited and fully auditable.

10.1.10. ensure that Supplier Personnel are informed of what constitutes acceptable access of operational or IT technology, Data and networks and the consequences of non-compliance.

10.2. For physical access the Supplier shall:

10.2.1. Implement and maintain a CCTV system to monitor the external building elevations, the main reception area, any other personnel entrance points, the goods delivery point(s), the external fire exit doors from the building and the entry / exit point into the area(s) processing the TfL Data. The System shall maintain a minimum of 30 days recording.

10.2.2. ensure external lighting for the building shall support any external elements of the CCTV system and give sufficient lighting for natural observation. Where this is not possible the CCTV system shall include infra-red lighting.

10.2.3. ensure that physical access to the areas used to process or store TfL Data shall be physically controlled (e.g. electronic access control system).

10.2.4. ensure that access to the areas processing or storing TfL Data should be restricted to those people working on the Services or those who have an operational requirement to access the area.

10.2.5. implement an electronic access control system to control and manage access into the building and internal areas used to process and store TfL Data. The System should log all activities, alarms and events and hold data for a minimum of 90 days.

10.2.6. define and document procedures to manage visitor and temporary access into the building and internal areas used to process and manage TfL Data.

11. Compliance

11.1. The Supplier shall have a documented compliance plan and conduct regular reviews (at least annually) to ensure that the security of TfL Data cannot be compromised.

11.2. TfL may require the Supplier to assist with TfL's Cyber Security assessment process. This may result in a full physical and logical information security review at all relevant locations in accordance with the Right to Audit section of the Agreement

11.3. Unless otherwise stated, the Supplier must respond to any requests for information or Data to be provided to TfL in relation to the Supplier Services within 30 days of notice.

12. Business Continuity

12.1. The Supplier shall provide a Business Continuity Plan that demonstrates how they will maintain the contracted service level in the event of an emergency. The Business Continuity Policy and Business Continuity Plan must align with the best practice detailed in the standard ISO/IEC 22301 Business Continuity Management.

12.2. The Supplier's Business Continuity Policy and Business Continuity Plan will be subject to an annual review by the Supplier and the updated documents will be shared with TfL no more than 12 months following the previous submission. TfL, acting reasonably, reserve the right to request further information relating to the Supplier's Business Continuity arrangements, including but not limited to exercise schedules and reports, and the Supplier will make all efforts to respond promptly to such information requests.

13. Security Reporting

The Supplier shall provide communicating metrics about security, risk, and the performance of security controls to TfL.

Supplier Reporting	**Timeframe for submission to TfL**
Security Management Plan	Within 20 days of the Contract Commencement Date.
Security Risk Assessment Methodology	Within 20 days of the Contract commencement date, and when significant changes to this document occurs.
Joiners, Movers & Leavers Notification	Every 3 months the Supplier will provide TfL a report on all Supplier Personnel who have joined or left the delivery of the Services provided to TfL.
Security Risks within the Risk Register	Within 3 months] of the Contract commencement date, and then at least 5 Business Days before each management meeting.
Security Risk Treatment Plan	Within 3 months of the Contract commencement date, and then at least 5 Business Days before each management meeting.
Security Risk Status Reports	Monthly from the Service commencement date and throughout the remainder of the Term of the Contract.
Penetration Test Report	At least annually following the Service commencement date, or within [two (2) months] following each significant change to the System or Assets (whichever is the sooner).
Wireless Access Point Scan Reports	Within 3 months] of the Contract commencement date, and then every three 3 months.
Review of actions following each Security Incident	Within 1 month] after each Security Incident and each Information Security Event (following the Service commencement date)

Security Improvement Plan	At least annually following the Service commencement date or within [one (1) month] following the identification of significant new vulnerabilities or threats (whichever is the sooner).
Review of Security Controls	At least annually following the Service Commencement Date.
Review of the corrective and preventive actions	At least annually following the Service commencement date.

ANNEX 2 – Definitions

Security Management Plan	means the Service Provider's security plan developed and revised pursuant to Paragraph 3.
Cyber Essentials Scheme	means the UK government scheme encouraging organisations to adopt good practice in information security, focussing mainly on technical controls rather than governance, risk, and policy.
Vulnerability Management	Vulnerability management is the various processes, tools, and strategies of identifying, evaluating, treating, and reporting on security vulnerabilities and misconfigurations within an organisation's software and systems.
Network & Information Systems (NIS) Directive	Network & Information Systems (NIS) is intended to establish a common level of security for network and information systems.
Business Continuity Plan	A Business Continuity Plan helps a company survive and continue running after a major disruption or disaster. It highlights the step-by-step process of what should be done to prevent risks that can lead to a business having to close.
Intrusion Detection System (IDS)	An Intrusion Detection System (IDS) is a monitoring system that detects suspicious activities and generates alerts when they are detected.
Intrusion Prevention Solution (IPS)	An intrusion prevention system (IPS) is a network security tool (which can be a hardware device or software) that continuously monitors a network for malicious activity and takes action to prevent it.
Asset Hardening and Secure Configuration	Asset Hardening and Secure is the process of reducing the attack surface of an Service Asset.
Cloud Services	Cloud Computing Services is the delivery of computing services including servers, storage, databases,

	networking, software, analytics, and intelligence over the Internet
Incident Management Plan	An Incident management Plan is a series of steps taken to identify, analyse, and resolve critical incidents, which could lead to issues in an organisation if not restored.
TfL Data	means data created, generated or collected, during the performance of the Services (or any part thereof), including Personal Data and data supplied to TfL and members of the TfL Group in connection with the Services or this Agreement.
Good Industry Practice	means the exercise of that degree of skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced service provider engaged in the same type of undertaking under the same or similar circumstances.
File-Integrity Monitoring	File Integrity Monitoring is used to monitor and alert changes to Data files.
Service Asset Register	means a register of all Information Assets relating to the Services connected to this Schedule.
ISO/IEC 22301	means the proposed standard that specifies security requirements for disaster recovery preparedness and Business Continuity Management Systems (BCMS).
Payment Card Industry Data Security Standard (PCI DSS)	The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards formed in 2004 by Visa, MasterCard, Discover Financial Services, JCB International and American Express.
Cardholder Data	Cardholder data (CD) is any personally identifiable information (PII) associated with a person who has a credit or debit card. Cardholder data includes the primary account number (PAN) along with any of the following data types: cardholder name, expiration date or service code.
Attestation of compliance (AoC)	An attestation of compliance (AoC) confirms that the RoC is accurate.

Report on Compliance (RoC)	A RoC is an assessment that determines PCI compliance.
ISO/IEC 27001	means the information security standard specification for an Information Security Management System (ISMS), with an emphasis on measuring and evaluating how well an organisation's ISMS is performing.
Security Incident	means a potential or actual event or attempted breach of security affecting the confidentiality, integrity or availability of the Service which processes or holds TfL Data.
Security Policy	means any TfL security policies as amended by TfL from time to time.
Security Risk	meaning all risks associated with the security of the Services which may have a negative impact upon the agreed security posture, including information security and any risks identified pursuant to the Security Management Schedule.
Security Risk Register	means a register of Security Risks produced and maintained as detailed in paragraph Security Principles 2.2.2.
Service Assets	means all assets and rights including all physical assets, Software, IPR, as well as spares and components whether in storage, repair or on sites, used by the Service Provider to provide the Services in accordance with this Agreement;
Log File	A log file is a computer-generated data file that contains information about usage patterns, activities, and operations within an operating system and/or , application.
Service Provider Personnel	means all employees, agents, consultants and contractors of the Service Provider or of any Sub-Contractor

Service Provider Premises	means any land or building where the Service Provider carries out any part of this contract
Key Management	the activities involving the handling of cryptographic keys and other related security parameters (e.g., passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and destruction.
Risk Management	the process of identifying, monitoring and managing potential risks in order to minimize the negative impact they may have on an organisation.

ANNEX 3 – List of relevant Policies and Standards

TO BE PROVIDED BY TFL UPON REQUEST

P116 Information Technology Security Policy
- This policy defines TfL's requirements for managing Information Security.

P009 Operational Technology Cyber Security -Operations and Maintenance
- This policy defines TfL's requirements for Operations and Maintenance.

P008 Operational Technology Cyber Security -Projects and Upgrades
- This policy defines TfL's requirements for Projects and Upgrades.

P006 Operational Technology Cyber Security
- This policy defines TfL's requirements for Cyber Security in Operational Technology.

S1735 Information Technology Access Control
- This standard provides guidance on how employee access should be limited to different types of data.

S1736 Network Information Security
- This standard covers the security of all transmissions within an organisation's network.

S1740 Cryptography
- This standard covers best practices in encryption.

S1747 Physical and Environmental Security of TfL's Information Technology
- This standard describes the processes for securing buildings and internal equipment.

S1790 Information Security Asset Management
- This standard describes the processes involved in managing data assets and how they should be protected and secured.

S1791 Operational Information Security
- This standard provides guidance on how to collect and store data securely, a process that has taken on new urgency thanks to the passage of the General Data Protection Regulation (GDPR) in 2018.

S1793 IT System Acquisition, Development and Maintenance

- This standard detail the processes for managing systems in a secure environment.

S1794 Information Security Supplier Management

- This standard covers how an organisation should interact with third parties while ensuring security.

S1795 Information Security Incident Management

- This standard covers how an organisation should manage information security incidents.

S1796 Information Security Aspects of Business Continuity Management

- This standard covers how business disruptions and major changes should be handled.

S1797 Information Technology Compliance

- This Standard identifies what government or industry regulations are relevant to the organisation, such as ITAR.

S1771 Operational Technology Cyber Security -Projects and Upgrades

- This standard covers how Projects and Upgrades should be managed.

S1772 Operational Technology Cyber Security-Operations and Maintenance

- This standard covers how Cyber Security should be managed in Operations and when performing maintenance activities.

Electric Vehicle Infrastructure Delivery (EVID)
Tranche 2, Batch 1
Contract Ref No: tfl_scp_002468
Appendix L
Service Levels Reporting Template

Please refer to Annex 8 (*Service Levels*) to the Order Special Terms for details about the Service Levels.

The spreadsheet contains a reporting template for PI 2 'Incident Management', PI 3 'Contact Centre Availability', PI 4 'Queuing Time' and PI 5 'Correspondence'.

A template tab for PI 1 'Charge Point Availability' is not included within the spreadsheet. However, PI 1 'Charge Point Availability' data should be reported as per paragraph 6.4.7 (Outage Events file) of the Order Specification.

Date	Incident Number	SLA Incident Timescale to resolve (refer to SLA)	Incident Detail	Chargepoint ID/Reference	Incident Time (hh:mm:ss)	Incident Resolved Date (YYYY-MM-DD)	Incident Restored Time (hh:mm:ss)	Incident Duration ((hh:mm:ss)	Comments

Date	Time Available From (hh:mm:ss)	Time Available to (hh:mm:ss)	Time Available (%)	Time Unavailable from (hh:mm:ss)	Time Unavailable to (hh:mm:ss)	Time Unavailable (%)	Comments

Daily availability logs

Date	Total Number of calls received	Calls answerd in 90 seconds	Percentage of calls answered in 90 seconds	Number of Calls not ansered in 90 seconds	Percentage of calls not answered in 90 seconds	Number of Calls answered in 240 seconds	Percentage of calls answerd in 240 seconds	Number of Calls not answered in 240 seconds	Percentage of calls not answerd in 240 seconds	Comments

Daily queuing time logs

Date	Total number of corrispondence received	Number of Responses provided within 5 working days	Percentage of Responses provided within 5 working days	Number of Responses not provided within 5 working days	Percentage of Responses not provided within 5 working days	Comments

Transport for London

Invitation to Quote

Electric Vehicle Infrastructure Delivery (EVID)
Tranche 2, Batch 1

Volume 2

Appendix M

Guide to Roadworks Assessment and Approvals

COMMERCIAL IN CONFIDENCE

TfL Restricted

Guide to Roadworks Assessments and Approvals

Network Management
March 2021



EVERY JOURNEY MATTERS

Guide to Roadworks Assessments and Approvals

1. Who is this guidance for? 3
2. Introduction to Network Management 4
3. Where do I start? 5
4. What do I do next? 6
5. What is a TMAN? 8
6. Scheme TMANs 9
7. Forward Plan Notice 10
9. Attached Works TMANs 12
10. Standalone Works TMANs 15
11. Traffic Regulation Orders (TROs) 17
12. Provisional Advance Authorisations (PAAs) 19
13. Permits 20
14. FPNs for Roadworks Offences 21
15. If you need more help 22
16. Abbreviations 23

1. Who is this guidance for?

This guidance is for TfL's project managers in Project and Programme Delivery and contractors wishing to undertake roadworks on TfL's roads and London's strategic road network.

It is intended to give clear guidance and advice about how to get roadworks assessed and approved, and how Network Management can support planning and execution of safe, efficient and sustainable works.

2. Introduction to Network Management

Network Management (NM) carries out TfL's Traffic Manager responsibilities on behalf of the Traffic Manager, Glynn Barton. NM manages the Transport for London Road Network (TLRN) and has strategic oversight of the Strategic Road Network (SRN).

NM is responsible for upgrading, monitoring and maintaining TfL's road and structural assets. Teams assess and co-ordinate schemes, road and street works, highway licences and events on the TLRN and manage most of London's traffic signals. The network in managed in real-time by the Network Management Control Centre (NMCC).

NM Teams work collaboratively with all areas of TfL as well as external organisations including the Boroughs, utility companies and major infrastructure project promoters.

3. Where do I start?

3.01 To submit a Provisional or Formal Traffic Management Act Notification (TMAN) application, you will need access to LondonWorks. Email **londonworks@tfl.gov.uk** to request "promoter access". As a LondonWorks user, you will also be able to apply for a Traffic Regulation Order (TRO) or Temporary Traffic Regulation Order (TTRO) using the Traffic Order Management System (TOMS).

3.02 Submission of a Forward Planning Notice, Provisional Advance Authorisation (PAA) or Permit Application, will be done via Street Manager. Your colleagues will be best placed to ensure you have access and to instruct you how each application can be made.

3.03 Through your early engagement with the Network Impact Specialist Team (NIST), schemes will be notified to the relevant Major Projects Co-ordination Group and details may be shown on NM's visual management provision. Early liaison with the Co-ordination, Assessment and Permitting Team (CAP) on works that are not scheme-related (Standalone Works) may also be notified to the Major Projects Co-ordination Group.

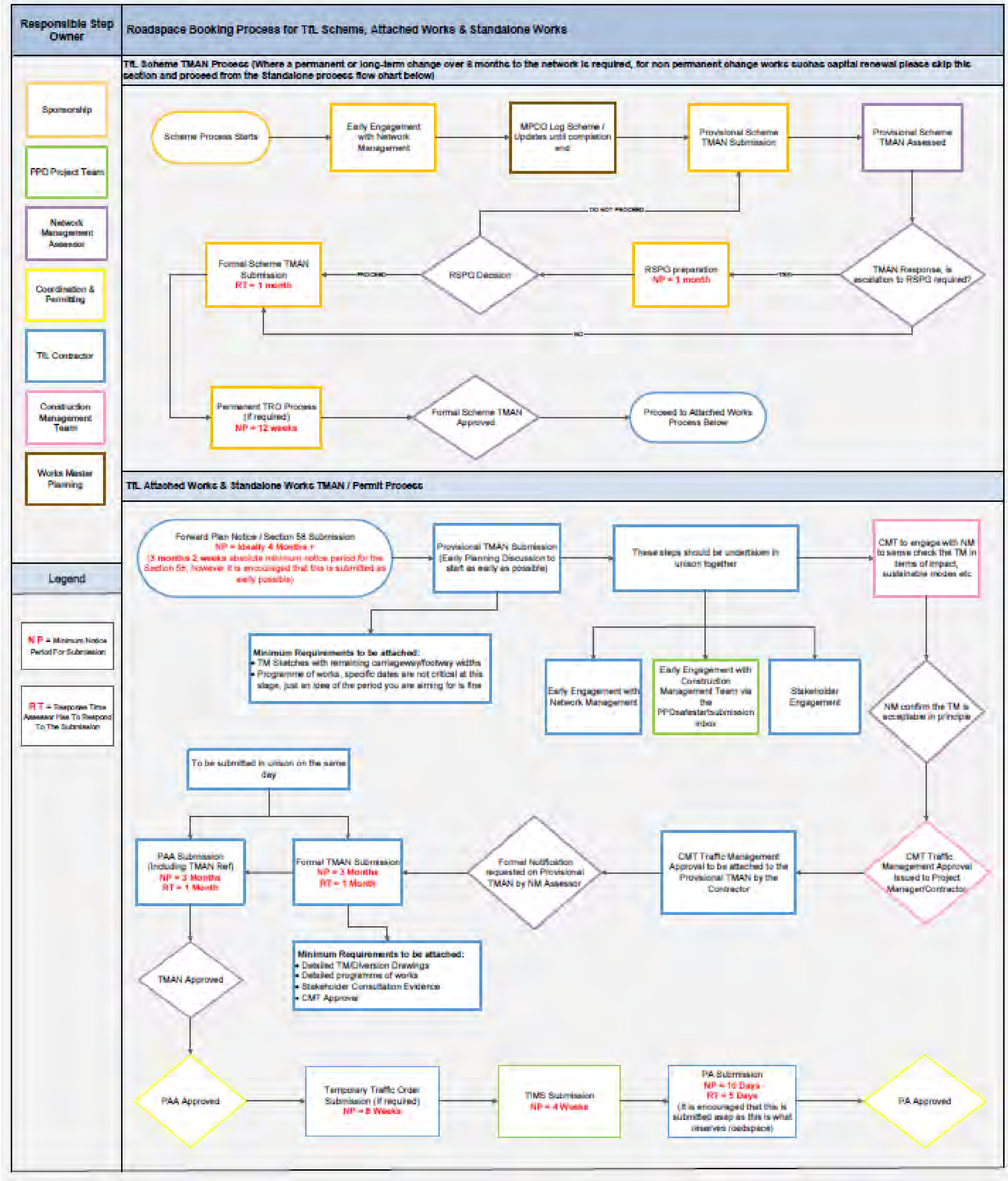
3.04 A Traffic Information Management System (TIMS) entry is required for all major works for discussion at the weekly Surface Assurance Meeting (SAM) for works in progress or starting in the following 10 days.

3.05 An initial co-ordination check using LondonWorks may help you see whether there are other works planned in the same location. This could help to identify collaborative opportunities for works promoters to work within the same space.

3.06 Promoters should check if their works will be subject to Lane Rental charges as these will add to the cost if works are proposed at traffic-sensitive times.

4. What do I do next?

The diagram below shows the main tasks, submissions and approvals for schemes, scheme-associated works and standalone works. These are following by what you need to do for each application.


Responsible Step Owner
Roadspace Booking Process for TfL Scheme, Attached Works & Standalone Works
Sponsorship
PPD Project Team
Network Management Assessor
Coordination & Permitting
TfL Contractor
Construction Management Team
Works Master Planning
Legend
NP = Minimum Notice Period For Submission
RT = Response Time Assessor Has To Respond To The Submission
TfL Scheme TMAN Process (Where a permanent or long-term change over 6 months to the network is required, for non permanent change works suchas capital renewal please skip this section and proceed from the Standalone process flow chart below)
Scheme Process Starts
Early Engagement with Network Management
MPCC Log Scheme / Updates until completion and
Provisional Scheme TMAN Submission
Provisional Scheme TMAN Assessed
DO NOT PROCEED
TMAN Response, is escalation to RSPG required?
YES
RSPG preparation
NP = 1 month
RSPG Decision
PROCEED
Formal Scheme TMAN Submission
RT = 1 month
NO
Permanent TRO Process (if required)
NP = 12 weeks
Formal Scheme TMAN Approved
Proceed to Attached Works Process Below
TfL Attached Works & Standalone Works TMAN / Permit Process
Forward Plan Notice / Section 58 Submission
NP = Ideally 4 Months +
(3 months 2 weeks absolute minimum notice period for the Section 58, however it is encouraged that this is submitted as early possible)
Provisional TMAN Submission (Early Planning Discussion to start as early as possible)
These steps should be undertaken in unison together
CMT to engage with NM to sense check the TM in terms of impact, sustainable modes etc
Minimum Requirements to be attached:
• TM Sketches with remaining carriageway/footway widths
• Programme of works, specific dates are not critical at this stage, just an idea of the period you are aiming for is fine
Early Engagement with Network Management
Early Engagement with Construction Management Team via the PPDsafestartsubmission inbox
Stakeholder Engagement
NM confirm the TM is acceptable in principle
To be submitted in unison on the same day
PAA Submission (Including TMAN Ref)
NP = 3 Months
RT = 1 Month
Formal TMAN Submission
NP = 3 Months
RT = 1 Month
Formal Notification requested on Provisional TMAN by NM Assessor
CMT Traffic Management Approval to be attached to the Provisional TMAN by the Contractor
CMT Traffic Management Approval Issued to Project Manager/Contractor
Minimum Requirements to be attached:
• Detailed TM/Diversion Drawings
• Detailed programme of works
• Stakeholder Consultation Evidence
• CMT Approval
TMAN Approved
PAA Approved
Temporary Traffic Order Submission (if required)
NP = 8 Weeks
TMS Submission
NP = 4 Weeks
PA Submission
NP = 10 Days
RT = 5 Days
(It is encouraged that this is submitted asap as this is what reserves roadspace)
PA Approved

5. What is a TMAN?

5.01 A TMAN is a Traffic Management Act Notification submitted by a TfL internal works promoter or a London borough via the LondonWorks portal where all documentation for your proposals can be assessed.

5.02 TMANs are assessed by the following teams:

Type of TMAN	Intervention	Assessment Team
Scheme TMAN	Permanent change to the network or a long term temporary arrangement	Network Impact Specialist Team
Attached Works TMAN	Temporary traffic management arrangements to construct a scheme	Network Impact Specialist Team
Standalone Works TMAN	TfL works that are not scheme-related and will have no permanent change to the network, such as capital renewal works, resurfacing, signal mods etc	Co-ordination, Assessment and Permitting Team

6. Scheme TMANs

6.01 A notifiable activity is one using Highways Act 1980 or Road Traffic Regulation Act 1984 powers. Parity is demonstrated as this requirement applies to TfL and the London Boroughs. Activities include:

Trigger:
Early engagement with NIST recommended

- A permanent change to the network
- Specific development-related works
- S278 works (Highways Act 1980)
- S6 (Road Traffic Regulation Act 1984)
- Major works that will significantly affect the operation of the Transport for London Road Network (TLRN), Strategic Road Network (SRN) or bus services
- S9 experimental schemes

6.02 The Project Sponsor is requested to engage the Network Impact Specialist Team (NIST) during the Feasibility stage of the project to discuss objectives and potential scheme options. Other TfL teams, such as the Lane Rental Team, will also be engaged at an early stage so the sponsor can decide on the best option to go through to Concept Design.

6.03 The Sponsor can submit a Provisional Scheme TMAN via LondonWorks based on those discussions and with a broad outline of the final project. This information can initially be quite vague, but detail and designs can be added to the TMAN as it progresses. NIST will provide ongoing guidance to ensure all necessary information is submitted and consultation is being progressed.

TMAN Trigger:
Submit Provisional Scheme TMAN

6.04 Continued liaison with NIST is important. When an operationally acceptable scheme has been agreed and the correct information is in place, NIST will request a Formal TMAN. The Sponsor can then convert the Provisional Scheme TMAN to 'Formal' status which requires an official response from NIST within 28 days of submission. The Formal TMAN should be a formalisation of agreements and plans and a formality for NIST to sign off. However, if plans are inaccurate or consultation has not been conducted, NIST **will** request revisions or supplementary information and TMAN approval progress will be delayed. See "What good looks like".

6.05 If the scheme requires a permanent change to the highway, a Traffic Regulation Order is required, and this can be requested with the approved Scheme TMAN number.

7. Forward Plan Notice

7.01 A Forward Plan notice is not compulsory, but is strongly encouraged. The proposed works will be visible on LondonWorks and will serve as a marker for co-ordination purposes in addition to identifying collaborative works opportunities. It can be submitted at any time and promoters are advised to submit in advance of a PAA. No TMAN reference is required.

8. Section 58

8.01 A Section 58 provides an enforceable restriction to protect the road following surfacing works. If a Section 58 restriction is required after the works are completed, this can be submitted on the Forward Plan notice specifying the restriction requirements/duration so that the relevant team can raise the Section 58 notice.

8.02 A minimum of 3 months and 2 weeks' notice is required. It is then sent to all works promoters to advise them there will be a restriction in place on that specific road which then gives them time to undertake their works before the restriction comes into force. See the Step-by-Step Guide.

9. Attached Works TMANs

9.01 Attached Works TMANs are for post-scheme approval and should be submitted as attached works to the Scheme TMAN.

9.02 On completion of Concept Design (Pathway Stage 3), PPD will be informed of scheme construction requirements when a Task Resource Order is received.

Trigger:
Early engagement with NIST recommended

9.03 A PPD Project Manager will be assigned and will define broad milestones.

9.04 The Project Manager will inform the highways contractor of the scheme and delivery milestones. The contractor will then be required to develop plans for construction.

9.05 Early engagement with NIST will help the Project Manager and contractor to consider various aspects of successful delivery, but in advance, a contractor should consider the following questions:

Questions for promoters

Approvals / Consents

- Will my proposals involve a TTRO – temporary traffic orders have an 8-week lead time. Does my diversion route create any challenges with neighbouring authorities or vulnerable assets?
- Have I carried out early engagement with NIST and submitted a provisional TMAN? This engagement will provide early awareness of proposals and help to ensure that significant issues are identified and addressed early on in the process.

Co-ordination

- Have I carried out an early co-ordination check with regard to neighbouring projects and determined this is an appropriate time to bring forward my proposed TM? How have I amended my TM / programme in light of neighbouring projects?

Do I need any or all of the following:

- **RSA report** (Road Safety Audit) for larger projects
- **SIR** (Scheme Impact Report) for larger projects
- **Modelling** (with approved level of impacts) that has been audited and finalised
- **Operational Readiness Report** (in the case of significant temporary change to the network
- **Traffic counts / accident data / other data** to justify designs to all stakeholders
- **TA report** (Technical Assurance) for development-related works
- **CLP** (Construction Logistics Plan) for development-related works and other street activities
- **CPOS support (Compliance, Policing and On-Street Services)**

Questions for promoters

Stakeholder Engagement

- Have I identified all of my key stakeholders and achieved buy-in to my proposals?
- Are my TM plans presented in a logical sequence and easy to interpret by all those who will be reviewing them?
- Have I engaged with TfL Communications / Travel Demand Management (TDM) and developed a communication plan where necessary?

TM / Design Considerations

- Have I designed my traffic management (TM) in accordance with the TfL TM handbook (See Section 8 of this guidance document)? This is mandatory on the TLRN and encouraged on SRN.
- Have I reviewed existing network conditions and made sure the TM I'm proposing best reflects prevailing demand?
- Do I need to use temporary signals as part of this proposal? Have I made contact with the necessary parties in TfL Network Management as the use of temporary signals, especially the Urban Traffic Control (UTC) variant, may involve significant lead times?
- Are my works likely to require a Variable Message Sign (VMS) strategy and have I developed one?

Level of Service / Safety

- How am I protecting and delivering a good level of service for pedestrians through my TM design?
- How am I protecting and delivering a good level of service for cyclists through my TM design?
- How am I protecting bus operations through my TM design?
- How have I gone about ensuring the TM represents the correct operational balance on this part of the network?

9.06 Traffic Management Plans will be scrutinised by the Construction Management Team in PPD to ensure they are fit for purpose.

9.07 A Provisional Works TMAN may be submitted with approximate details and plans. These can be refined in line with discussions and agreements to deliver best practice.

9.08 It is important that a Works TMAN has the same title as the approved Scheme TMAN and references the Scheme TMAN number. This ensures clarity that the works are linked to a scheme and avoids any confusion with assessment teams.

9.09 For complex or multiple-phased projects, the Works TMAN will need to define each phase with a clear TM plan and timings. For longer term projects, it might even be necessary to submit more than one Works TMAN during construction.

9.10 NIST will assist at all stages of the notification process. Promoters are asked to liaise with the respective Network Impact Manager throughout the process to help ensure that submissions are processed as efficiently as possible.

9.11 An informal discussion with the Co-ordination, Assessment and Permitting (CAP) is recommended, so they are aware of the works proposals. A Forward Plan may also be submitted through LondonWorks as advance notice of works. This is just an indicator that works are being proposed and does not guarantee construction dates.

9.12 At the point when all aspects have been considered and addressed, TM plans are accurate with corresponding construction and phasing plans, stakeholder consultation has been concluded and all agreements secured, NIST will advise the promoter to convert the Provisional Works TMAN to "Formal" status. NIST approval should therefore be a formality as the Formal Works TMAN should be an accurate representation of discussions, plans and agreements.
Note: It is the promoter or contractor's responsibility to ensure all information and plans are accurate.

9.13 NIST aims to ensure that all notifications for works affecting the TLRN / SRN are processed in a timely fashion. This helps to ensure that the network continues to operate as efficiently as possible, in line with TfL's statutory obligations, whilst helping to meet proposed delivery programmes.

9.14 When the Works TMAN is approved, a decision letter will be sent to the promoter and may contain working conditions. The letter will also advise if Lane Rental charges will apply. The TMAN reference can be used to apply for Temporary Traffic Order(s) (TTRO) if applicable and a Provisional Advance Authorisation (PAA) for initial co-ordination. Any conditions specified on the Works TMAN should be applied to any TTROs, PAAs and Permit applications.

9.15 For best practice on safety around works, see TfL's Temporary Traffic Management Handbook and Safety at street works and road works: a code of practice 2013.

10. Standalone Works TMANs

10.01 Works that are not scheme-related and do not have a permanent change to the network are classified as Standalone Works, for which a TMAN is required and will be assessed for impact and initial co-ordination purposes by CAP. Generally, low impact minor works permits would not require a TMAN, however this is site specific and CAP can advise if in doubt.

10.02 Examples of Standalone Works are as follows:

- Drainage works
- Footway renewals
- Signal modifications
- Red light/speed cameras
- Scoot renewals/repairs
- Regular maintenance works
- Block closures
- Capital renewal works eg resurfacing
- Topographical surveys
- Highways England works (predominantly for diversions)
- Borough standalone works that affect the TLRN or SRN

10.03 Minimum requirements for a Provisional Standalone Works TMAN:

A Provisional Works TMAN may be submitted with approximate details and plans. These can be refined in line with discussions and agreements to deliver best practice.

10.04 Traffic Management Plans will be scrutinised by the Construction Management Team to ensure they are fit for purpose.

10.05 A Provisional Standalone Works TMAN can be submitted for early information and initial co-ordination purposes.

10.06 When all the information is correct, the status of the TMAN can be promoted to "Formal" and will be assessed within 28 days by CAP.

10.07 **Minimum requirements for a Formal Standalone Works TMAN**:

- Programme with accurate phasing (see Traffic Management Schedule)
- TM drawings to be sufficient quality for assessment
- CMT approval
- Confirmation of stakeholder consultation
- Clear and agreed diversion routes

- Bus provisions
- Cycling and pedestrian management provisions
- Accessibility provisions
- Acknowledgment of the requirement of any TTROs, suspensions etc.

10.08 For best practice on safety around works, see TfL's Temporary Traffic Management Handbook and Safety at street works and road works: a code of practice 2013.

10.09 A PAA may be submitted at the same time as a Formal TMAN, but will not be approved until the Formal TMAN is approved.

11. Traffic Regulation Orders (TROs)

11.01 A TRO is a legal document under the Road Traffic Regulation Act 1984 and is needed if works, maintenance or permanent change is required on the TLRN.

TRO Trigger:
Provide initial information with existing and new road layout to STOT

Timescale: At least 98 days before scheme completion

11.02 Applications can be made via TOMS on LondonWorks. The system will prompt you to provide the relevant information for your TRO and your TRO will remain in your Dashboard until it has been completed.

11.03 To obtain access to TOMS in LondonWorks, you will need to apply for access through your Project Manager. Once this access is granted, you will be directed to the Streets Traffic Orders Team (STOT) to receive training on TOMS and to be instructed how to submit orders for drafting and processing.

11.04 Temporary Traffic Regulation Orders are required for:

- Road closures
- Banned Turns
- Utility Works
- Suspensions (for 24 hour suspensions only)

11.05 Temporary Consolidated Suspension Requests (TCSR) may be submitted, where the suspension is within the base restriction for the Red Route, i.e. 7am-7pm, 8am-7pm etc.

11.06 Bus Lanes have built in exemptions for suspending them and do not always require a TTRO or a TCSR.

11.07 PTRO (Permanent Traffic Regulation Order) and ETRO (Experimental Traffic Regulation Orders) applications are required when a TTRO is required for a change/amendment/implementation to the TLRN. It is the Sponsor's responsibility to apply for the PTRO or ETRO.

11.08 There are timelines for the implementation of these section types, to permit drafting, statutory consultation and statutory processing to take place as governed by Act and Legislation. These requirements are built into our processes and the required timelines are:

- PTRO requires 12 weeks' lead time
- ETRO requires 12 weeks' lead time
- TTRO requires 8 weeks' lead time
- TCSR requires 3 weeks' lead time

11.09 These timelines can change dependent upon the need for a works order when implementing a permanent or experimental fixture, because the 8 weeks works order needs to be built in the 12 weeks lead time. There is an opportunity for these timelines to run in parallel when implementing a permanent and temporary scheme which requires a work order. It is recommended that a discussion takes place with the STOT team to facilitate this.

11.10 A TMAN, Permit and PAA will need to be applied for prior to the traffic order application. You cannot register your traffic order until these item reference numbers have been achieved. You will be able to record your entry and save it, but will not be able to submit it until all of this information has been inputted.

12. Provisional Advance Authorisations (PAAs)

12.01 The lead time for a PAA is 90 days with a response time of one calendar month.

12.02 The PAA does not reservice the roadspace. The granting of a PAA co-ordinates and provisionally books works in, pending subsequent approval of the Permit.

12.03 The promoter must quote a Formal TMAN Works application reference in the model condition box. The TMAN does not need to be approved at this stage, just submitted.

Roadspace is not reserved until the Permit has been granted

12.04 It is encouraged that the promoter contacts the CAP coordinator once the TMAN is approved so they are aware that the PAA can now be responded to (when they have the opportunity to do so), as otherwise this may not be picked up until the PAA "respond by" date.

12.05 Statutory application and response times as described in the London Permit Scheme (LoPS) Section 8.4.9 are shown in the table below.

Application and Response Times

ACTIVITY TYPE	Minimum application periods ahead of proposed start date		Minimum period before Permit expires for application for variation (including extension)	Maximum response times		Response times to applications for Permit variations
	Application for Provisional Advance Authorisation	Application for Permit		Application for Provisional Advance Authorisation	Application for Permit	
Major	3 months	10 days	2 days or 20% of the original duration whichever is longest	1 calendar month	5 days	2 days
Standard	n/a	10 days		n/a	5 days	
Minor	n/a	3 days		n/a	2 days	
Immediate	n/a	2 hours after		n/a	2 days	

13. Permits

13.01 A Formal Works TMAN must be approved prior to a Permit application.

13.02 The Permit application must quote the TMAN reference and list the model conditions applied in the Decision Letter provided on the Works TMAN.

13.03 A Permit application should be submitted a minimum of 10 days prior to the proposed start of works, but the earlier, the better as this reserves the roadspace.

13.04 CAP will run a final co-ordination check and will grant the Permit if there are no network conflicts.

13.05 Statutory application and response times as described in the London Permit Scheme (LoPS) Section 8.4.9 are shown in the table below.

Application and Response Times

ACTIVITY TYPE	Minimum application periods ahead of proposed start date		Minimum period before Permit expires for application for variation (including extension)	Maximum response times		Response times to applications for Permit variations
	Application for Provisional Advance Authorisation	Application for Permit		Application for Provisional Advance Authorisation	Application for Permit	
Major	3 months	10 days	2 days or 20% of the original duration whichever is longest	1 calendar month	5 days	2 days
Standard	n/a	10 days		n/a	5 days	
Minor	n/a	3 days		n/a	2 days	
Immediate	n/a	2 hours after		n/a	2 days	

14. FPNs for Roadworks Offences

14.01 Network Regulation (NR) may give fixed penalty notices (FPNs) for specific roadworks offences, which include working without a permit, site-based failure to comply with permit conditions, or administrative non-compliances (eg late delivery of a notification).

14.02 FPNs will be given electronically (via Street Manager or equivalent API).

14.03 It is strongly advised that systems are checked regularly for FPNs so they may be reviewed and either challenged or accepted.

14.04 If challenged, representation must be made within 29 days of the date of issue of the FPN and should be made electronically using email or FPN comment.

14.05 A periodic report of FPNs ready for payment will be sent by NR to the TfL Budget Control team which will adjust the amount owed for those FPNs from the periodic payment application.

15. If you need more help

The following are linked to documents which you may find helpful:

TfL's Temporary Traffic Management Handbook

Safety at street works and road works: a code of practice 2013

Traffic Management Plan guidance

Section 58 Request Process for Promoters

TMANs – what good looks like

CPOS Service Level Agreement

Template:

Traffic Management Schedule

Contact lists:

NIST

STOT

CAP

Legislation links:

Traffic Management Act 2004

New Road and Street Works Act 1991

Traffic Regulation Act 1984

Highways Act 1980

Local Authorities' Traffic Orders (Procedure) (England and Wales) Regulations 1996

Road Traffic (Temporary Restrictions) Procedure Regulations 1992

16. Abbreviations

Abbreviation	Full name
API	Application Programming Interface
CAP	Co-ordination, Assessment and Permitting Team
CLP	Construction Logistics Plan
CMT	Construction Management Team
CPOS	Compliance, Policing and On-Street Services
ETRO	Experimental Traffic Regulation Order
FP	Forward Plan Notice
FPN	Fixed Penalty Notice
LoPS	London Permit Scheme
LW	LondonWorks
NIST	Network Impact Specialist Team
NM	Network Management Directorate
NMCC	Network Management Control Centre
NPD	Network Performance Delivery
NR	Network Regulation
NRSWA	New Road and Street Works Act 1991
PA	Permit Application
PAA	Provisional Advance Authorisation
PPD	Project and Programme Delivery
PTRO	Permanent Traffic Regulation Order
RSA	Road Safety Assessment
SIR	Scheme Impact Report
SRN	Strategic Road Network
STOT	Streets Traffic Orders Team
TA	Technical Assurance Report
TCSR	Temporary Consolidated Suspension Request
TDM	Travel Demand Management
TLRN	Transport for London Road Network
TM	Traffic Management
TMA	Traffic Management Act 2004
TMAN	Traffic Management Act Notification
TOMS	Traffic Order Management System
TRO	Traffic Regulation Order
TTRO	Temporary Traffic Regulation Order
UTC	Urban Traffic Control
VMS	Variable Message Sign

Transport for London

Invitation to Quote

Electric Vehicle Infrastructure Delivery (EVID)
Tranche 2, Batch 1

Volume 2

Appendix N

Site Standards

COMMERCIAL IN CONFIDENCE

TfL Restricted

MAYOR OF LONDON

TRANSPORT FOR LONDON
EVERY JOURNEY MATTERS

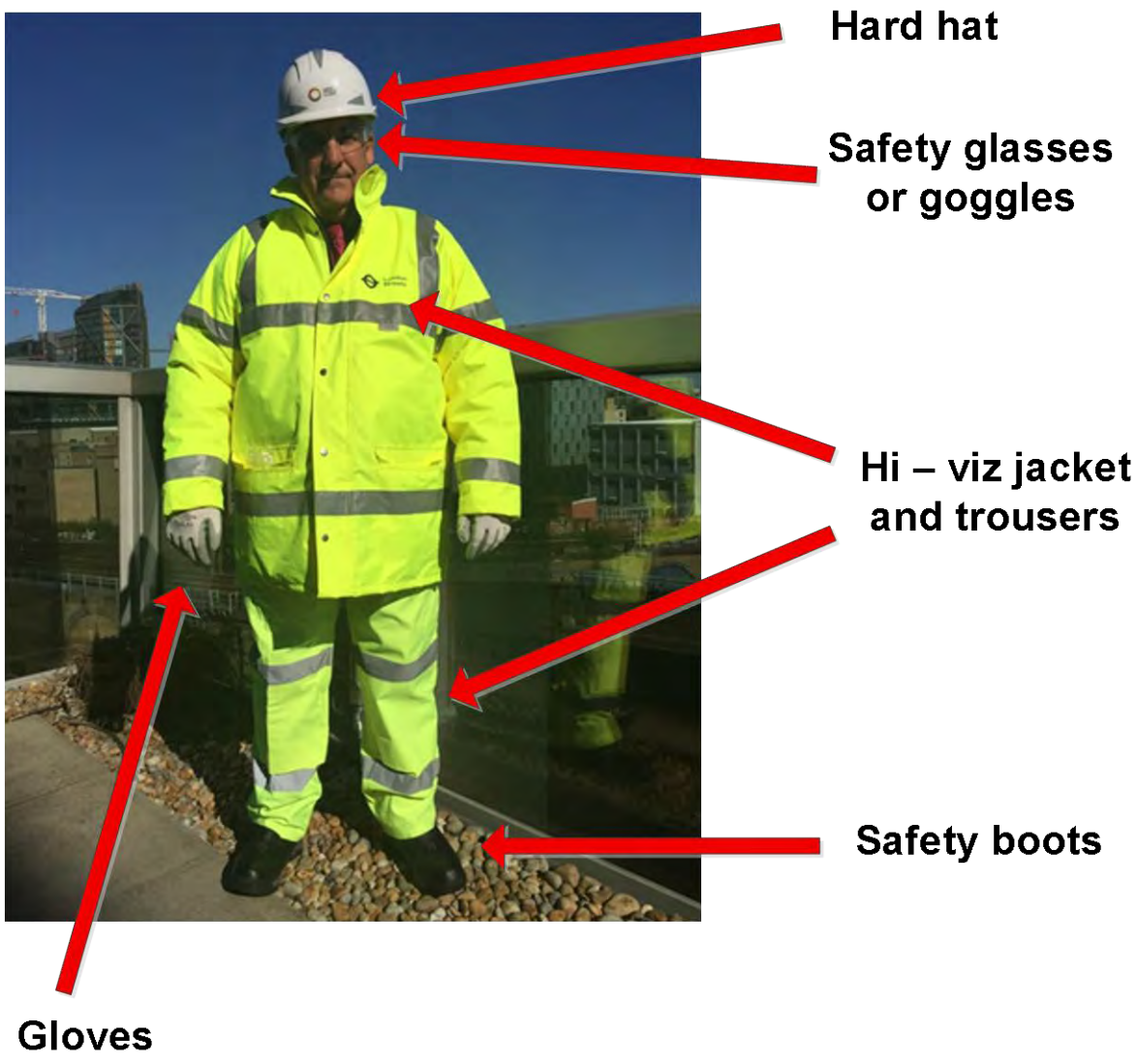
PPD Site Standards



PPE

PPE **MUST** be worn when entering any live sites, if you do not comply to these health and safety regulations you can be refused entry.

The minimum requirements for PPD sites are:



CSCS Cards

Anyone attending site should have a CSCS card, you can book your training through the CITB website:

http://www.citb.co.uk/cards-testing/health-safety-environment-test/

You can claim back on your test through expenses, which will be signed off by your line manager.

Barriers

Works are generally protected by 1.2m, half height barriers, need to be clipped together.

Barriers can be unclipped to allow access to the works area but must be re-clipped once personnel or materials are taken in or out of the works area. White metal barriers can be used on the footway side for pedestrian management





Plastic barriers (which are generally red but can be green or blue depending on contractor) clipped together to be used road side with road traffic cone to provide sideways safety zone. Barriers are to be secured to prevent them from being blown over. The pedestrian route should maintain 2.0m width where possible. Pinchpoint are inevitable but these should be kept to a minimum. Routes should be as direct as feasibly possible to avoid unnecessary delay to the public moving through the area but without compromise to safety.

There works are being carried out for extended periods or there are excavations and better protection is required 2.0m high Heras style fencing is to be used. Red and white retroreflective barriers can be secured to the fencing where there is insufficient road space to accommodate water filled barriers. These barriers are to be doubled clipped and braced as appropriate. All site compounds and material stores should be protected in this manner with lockable gates as appropriate. All site access point to be closed as soon as is practically possible.

Barriers should **NOT** look like this





Where works require breaking or cutting activities ensure dust suppression methods are used and the public is suitable protected from potential debris conflict and excessive noise through the use of hoarding, acoustic barriers, debris netting





Traffic Signals

All temporary traffic signals (including pedestrian aspects) to have red and white shrouds and securely locked with excess cabling retained within the shroud. Pedestrian push buttons must be accessible. If shrouds cannot be used the temporary signals should be barriered off to avoid trip hazards but push button will need to be accessible.







Signage

All works to be clearly signed. Permit boards to be in place filled out with the correct information for the works.





PPD sites are to be sufficiently branded so it is clear who is carrying out the works and what the works are delivering.





Pedestrian signage should give clear directions to key locations i.e. Stations, Major Roads / Streets, Key Buildings and crossing points. Direction signage to roads / streets should only be given if the normal route of access is diverted or obstructed.

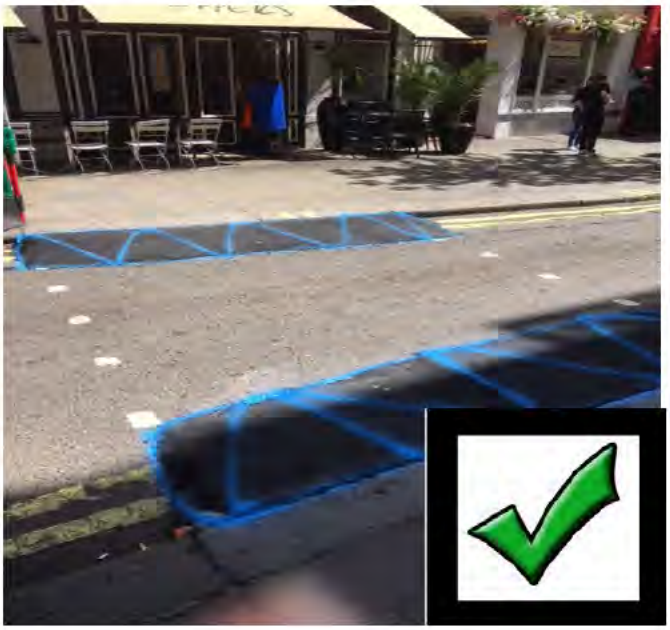
Signage and traffic management that is **NOT** acceptable





Ramps

If temporary ramps are required these should be a maximum of 1 in 12. Ramps can either be purpose made yellow GRP boards which must be pinned to the footway to avoid movement. Tarmac ramps must have a drainage pipe at the edge of the kerb to allow water to flow through and prevent ponding. Rubbish and debris should be cleared to prevent the blockage to the drainage pipe.



Transport for London

Invitation to Quote

Electric Vehicle Infrastructure Delivery (EVID)
Tranche 2, Batch 1

Volume 2

Appendix O

Cleaner Air for London Indent Logo

COMMERCIAL IN CONFIDENCE

TfL Restricted

Cleaner Air for London ident



Transport for London

Invitation to Quote

Electric Vehicle Infrastructure Delivery (EVID)
Tranche 2, Batch 1

Volume 2

Appendix P

Safe to Start Approvals List

COMMERCIAL IN CONFIDENCE

TfL Restricted

Rev 4

Safe to Start Approvals List

Name Project:	**PM:**
Programme of works:	**CMT:**
Project ID Number:	**PPP:**

TfL Pathway Stages	Permits or Consents	Required (Y/N)	Date Achieved	Comments
ADVANCE OR INVESTIGATORY WORKS (usually during FEASIBILITY or CONCEPT DESIGN Stages)	PPD Service Request (or PMSR)	**Mandatory**		
	CDP2 or TOR response submitted to contractor (one per Design Stage)	**Mandatory**		
	Project Task Order/ Call off Contract is submitted to contractor	**Mandatory**		
	Site visit with CMT, TAA and Contractor to agree core/ trial holes locations (if applicable)			
	Approach Bus Operations to agree possible bus mitigations (temporary during construction and permanent if the scheme affects journey times) and get measures' approval**			
	Written Borough and other stakeholders' agreement for Traffic Management proposals**			
	Planning Consent (if required)*			
	Private License Agreement (if required)*			
	TM review by CMT**			
	Noise Restrictions Check. Needed for Section 61**			
	Check whether scheme is in a HOT SPOT (anti-social behaviour)			
	Works Formal TMAN			
	TIMs submission **(min 4 weeks before site)** ***	**Mandatory**		
	Lane Rental Engagement to discuss possible waivers			
	Works Permits (PAA & PA) - for TfL and Borough's roads			
	Communications Plan/ Strategy (TDM & CCT Teams)			
	TTRO (Section 14-1) - **8 weeks before site** ****			
	Bus Stop suspensions (Bus Operations) - **min 2 weeks before site**			
	Site specific RAMS review by CMT			
	Bus Operations Notification for traffic diversions			
	CPOS Engagement (when relevant)			
	National Highways Approval (NOMS, TTRO, Departure, etc) (if required)			
	LU Approval (if required)			
	Section 8 (Powers & Consents) - **PPD Director's signature required**			
	Ensure Signal Contractor is booked for temp signals (if needed)			
	Contractor set up on Info Exchange			
	Residents Letter - for Road Network impactful schemes			
	Borough notification/ approva			

**NORMALLY ONLY RELEVANT TO RAPIDS*

***REQUIRED IN ADVANCE TO TMAN AND TTRO*

****Tick APPROVED cell if submitted*

***** If request from contractor is between 5 an 8 weeks, escalate via Programme Coordination Manager*

Programme Manager:

Signature:

Rev 4

Safe to Start Approvals List

Name Project:		**PM:**	
Programme of works:		**CMT:**	
Project ID Number:		**PPP:**	
Current Stage	STAGE GATE DETAILED DESIGN	**Gate**	4

TfL Pathway Stages	*Permits or Consents*	Required (Y and N & Mandatory)	Date Achieved	*Comments*
STAGE GATE 3 - CONCEPT DESIGN	PPD Service Request (or PMSR)	**Mandatory**		
	TAA Approval for CD (TfL Eng)			
	Buildability Approval for CD (CMT)			
	Utility Diversions Review (CMT) including Private Supply Surveys			
	Site visit with CMT, TAA and Contractor to agree core/ trial holes locations (if applicable)			
	Signal Design drawings/ Blue Spec/ Approved Equipment list and Power and Comms Requirements			
	RSA1 (if needed)			
	RSPG Approval (if required)			
STAGE GATE 4 - DETAILED DESIGN	PPD Service Request (or PMSR) issued by IDP/ Developer/ Boroughs	**Mandatory**		
	CDP2 or TOR response submitted to contractor (one per Design Stage)			
	Project Task Order/ Call off Contract submitted to contractor			
	Approach Bus Operations to agree possible bus mitigations (temporary during construction and permanent if the scheme affects journey times) and get measures' approval**			
	Written Borough and other stakeholders' agreement for Traffic Management proposals**			
	Planning Consent (if required)*			
	Private License Agreement (if required)*			
	TAA Approval for DD (TfL Eng)			
	Buildability Approval for DD (CMT)			
	RSA2 (TfL Eng) (if needed)			
	TM review by CMT**			
	Noise Restrictions Check. Needed for Section 61**			
	Check whether scheme is in a HOT SPOT (anti-social behaviour)			
	Works Formal TMAN			
	TIMs submission **(min 4 weeks before site)** ***	**Mandatory**		
	Lane Rental Engagement to discuss possible waivers			
	Section 58	**Mandatory**		
	Works Permits (PAA & PA) - for TfL and Borough's roads			
	Communications Plan/ Strategy (TDM & CCT Teams)			
	Permanent Traffic Orders (Required before TTRO submission)			
	TTRO (Section 14-1) - **8 weeks before site** ****	**Mandatory**		
	Bus Stop suspensions (Bus Operations) - **min 2 weeks before site**			
	Bus Operations Engagement in case bus shelters are affected			
	Site specific RAMS review by CMT - **min 14 days before site**			
	Environmental Impact Assessment (EIA) (if required)			
	Bus Operations Notification for traffic diversions - **12 weeks before site**			
	Engagement with Asset Operations Area Manager to ensure handover and for boundary changes (Highways and Traffic)			
	CPOS Engagement (when relevant)			
	National Highways Approval (NOMS, TTRO, Departure, etc) (if required)			
	LU Approval (if required)			
	Section 8 (Powers & Consents) - **PPD Director's signature required**	**Mandatory**		
	Section 17 notices issued (sites installed after 31/03/19)*	**Mandatory**		
	Residents Letter **- min 2 weeks before site**	**Mandatory**		
	Detailed Design Package Approved (including task price list, CDM documents, etc)	**Mandatory**		
	Utility Diversion's payment is made to allow programming of works			
	Ensure Signal Contractor is booked (if directly engaged by TfL)			
STAGE GATE 5 - DELIVERY	PPD Service Request (or PMSR) issued by IDP/ Developer/ Boroughs	**Mandatory**		
	Contractor set up on Info Exchange			
	Submit Project Task Order/ Call of Contract or Notice to proceed to Build Stage to contractors	**Mandatory**		

****NORMALLY ONLY RELEVANT TO NEW ELECTRIC CONNECTED ASSETS (ie. RAPIDS)***	**Programme Manager:**	
REQUIRED IN ADVANCE TO TMAN AND TTRO		
****Tick APPROVED cell if submitted***	**Signature & Date** :	
***** If request from contractor is between 5 an 8 weeks, escalate via Programme Coordination Manager***		
Reviewed by PPP Team and PMU Team*	**Signature & Date** :	

Transport for London

Invitation to Quote

Electric Vehicle Infrastructure Delivery (EVID)
Tranche 2, Batch 1

Volume 2

Appendix Q

EVID Contractor's Guide Traffic Orders, Notices and Suspensions

COMMERCIAL IN CONFIDENCE

TfL Restricted

Transport for London
Surface Transport

EVID Contractor's Guide

Traffic Orders/ Notices and Suspensions (TCSRs)

1 Purpose

If you intend to carry out a task on the TLRN, you may first require legal authorisation in the form of a Traffic Regulation Order / Traffic Notice, as specified by the Road Traffic Regulation Act 1984 (RTA). The Streets Traffic Orders Team (STOT) exists to support you by processing these legal documents on your behalf. This "Guide" will help you identify which Order / Notice type you require, and will inform you of STOT's associated timescales and processing requirements. For further guidance, please see the appendices.

2 Definitions

RTA - The Road Traffic Regulation Act 1984

STOT - Streets Traffic Orders Team

TCSR - Temporary Consolidated Suspension Request

TLRN - The Transport for London Road Network

TRO - Traffic Regulation Order

TTRO - Temporary Traffic Regulation Order

3 Statutory Requirements and Timeframes

The RTA sets out the statutory requirements with which TfL must comply before certain activities may be legally undertaken on the TLRN. For example, the public must first be consulted regarding any permanent changes to the network, and any objections raised will require a formal response before permission to proceed can be granted. Moreover, these consultation periods, and their outcomes, must be advertised in local newspapers, which have their own press deadlines. Consequently, the processing time for Traffic Regulation Orders / Notices can be substantial. Please engage with STOT early, to ensure there is enough time to meet the statutory requirements. It is important to get this right, as failure to comply can expose TfL to legal and reputational risk, and result in the delay or cancellation of works / schemes.

4. Traffic Regulation Order / Traffic Notice Types

There are 2 categories of TRO / Notice: Permanent and Temporary that will apply to EVID bays. This guide will help you identify the TRO / Notice type you require. Should you require any further type of TRO or have a query, you should contact STOT.

4.1 Permanent Orders / Notices:

To safeguard your scheme from legal risk, delay or cancellation, please ensure that your Permanent Order is in force before any activities are carried out which could be construed as related to a scheme (e.g. "preparatory works"

or “soft starts”). Otherwise, these actions could be interpreted as prejudging the outcome of any public consultation, and TfL could be challenged in court.

4.1.1 **Section 6** – for permanent changes to the network, including adding, changing, or removing bays of various types, bus lanes, prescribed routes, banned turns, weight restrictions, mandatory cycle tracks on the carriageway and lengths of double red, or wide red lines. Most orders for routine planned maintenance are now also done through Section 6 (Order for cleaning underpasses, tunnels, etc). Once STOT has received your Section 6 application, the processing time is 12 weeks.

NB: Other types of permanent Orders / Notices are available but are not widely used (e.g. Closure of footways, subways and footbridges). Please contact STOT if none of the permanent Order / Notice types described above meet your requirements.

4.2 Temporary Orders / Notices:

To facilitate planning and mitigate against risk, STOT invites promoters to specify two works periods for each Temporary Order application. This will provide flexibility should plans need to change at short notice. For example, if a crane operation were to be abandoned due to high winds, the work could be carried out the following weekend, if those “backup dates” had been specified in the original order. Otherwise, you would need to re-apply for an entirely new order, causing additional delay.

4.2.1 **Section 14(1)** – for temporary planned works that will require between several hours and 18 months to complete (although there are exceptions). For example, Section 14(1) would be used for an engineer to temporarily suspend bays, close roads, ban turns, put in temporary speed restrictions, weight restrictions, crane operations, etc. Once STOT has received your Section 14(1) application, the processing time is 8 weeks.

4.2.2 **Section 15(2)** – for temporary prohibitions or restrictions that are expected to last for longer than 18 months. When an original Section 15(2) Order is no longer required, a second Section 15(2) Order is required to revoke it. All Section 15(2) Orders require the publishing of a Notice of Intent. Once STOT has received your Section 15(2) application, the processing time is 8 weeks

4.2.3 **Section 14(2)** – for emergencies where urgent action or short-term restrictions are required. This Notice can be issued for litter clearing / street cleaning (available for up to 5 days) or because of damage or danger to the road (available for up to 21 days). Typical examples would include burst water mains, broken manhole covers, or anything needing immediate attention which could not be deemed planned works. Once STOT has received your Section 14(2) application, it will be processed immediately. However, notice should be given if possible. As only one additional 14(2) Notice can be issued for the same works, if a longer period will be required, a 14(2)-(1) should be requested.

4.2.4 **Section 14(2)-(1)** – for emergencies for which resolution is likely to require a considerable length of time. This Notice is an emergency 14(2) Notice

followed by a shortened procedure for implementing a 14(1) for continuation of the original Notice. Consequently, the work's duration can be extended to a maximum of 18 months. A typical example would a burst water main requiring contractors to be on site immediately, followed by significant works to restore the road to its original condition. Once STOT has received your Section 14(2)-(1) application, it will be processed immediately.

4.2.5 **TCSR suspension** – for suspending bus lanes at any time, or suspending parking bays between 7am-7pm Monday-Saturday. Please note that if you require a parking bay to be suspended outside the hours of 7am-7pm Monday-Saturday, then you should instead submit a Section 14(1) application. Once STOT has received your TCSR suspension application, the processing time is 3 weeks. Note however that bus lane suspensions at night do not cover 7am-7pm bays or single red lines, a section 14(1) would be required in this case.

NB: Other types of temporary Orders / Notices are available but are not widely used. Please contact STOT if none of the temporary Order / Notice types described above meet your requirements.

Prior to submitting any TRO, your order needs to go through an assessment process via Street Manager, TMAN and CaP. Until this has been done you CANNOT submit your TRO requests in TOMS. At Appendix D, is an example of a plan which should be submitted with your request in TOMS.

5. Traffic Orders Section

EVID Suppliers need to apply to Londonworks for access to submit TRO requests. This document sets out the information you will need to gain access to TfL bespoke systems, obtaining support and useful information for submitting fit for purpose requests:

5.1 ACCESS TO LONDONWORKS:

This will give EVID Suppliers access to the Traffic Order Management System (TOMS), a system required to make applications of all traffic orders to the Traffic Order Team.

You will need to do the following to have access:

Send email to londonworks@tfl.gov.uk requesting for TOMS access

With Full Name, Reason for TOMS access, contact number and organisation name.

You will need the login credentials that LondonWorks sends to you to log into TOMS

(LondonWorks will send you an email with your login credentials and a link, please follow this link to lunch into TOMS)

5.2 TRAINING

STOT to train EVID Supplier on how to use TOMS to apply for traffic orders.

EVID Supplier will register with Rohan Chandra to schedule training.

There is also a 'Train the Trainer option for the EVID Supplier, this an option that EVID Supplier may consider and discuss with Traffic Order Manager.

What our training will cover are the following:

- How to use TOMS for applications
- Types of plans and diversion plans that is acceptable to STOT Team
- Turn around delivery time

5.3 CONTACTING THE TEAM

For general requests send to the Traffic Order Section Mailbox (trafficordersection@tfl.gov.uk) which is monitored daily by the STOT Team. If you have already applied for a request in it will assign the request to the STOT representative (Appendix A) that covers that borough. They should be your only contact regarding the scheme and will be able to give you the support required.

STOT holds Drop-in Sessions (virtually on Tuesday and Thursday mornings between 9am and 12pm, to assist anyone having difficulty in submitting their Orders for processing). Please arrange by emailing TRO mailbox.

5.4 APPLYING FOR TRAFFIC ORDERS AND SUSPENSIONS

All statutory requests, whether TRO or TTRO Orders and Notices as well as TCSR suspension requests need to be inputted into TOMS system, any application made by email will be rejected on returned.

All temporary suspension requests (TCSR) will need to be received 21 days prior to the start date of the required suspension. Any suspension without 21 days advanced notice will also be rejected. 8 weeks advanced notice is required for a Section 14(1) Order. Please see 'Order Type Explanations' document for a full list of processing times.

The entire flow is captured in Appendix E.

5.5 TOMS

TOMS is the Traffic Orders system that allows anyone across TfL to make application for all types of orders/ notices and suspensions (TCSR). We only accept requests made through the TOMS system, it allows you to pick the type of request you want asking for road, dates, applicant and payment details, you can also add attachments/ plans. It will also advise of processing guidelines/ deadlines and costs.

The request should not be released in TOMS to STOT until:

- Applications have been through an assessment
- You have evidence of payment or Purchase Order
- You have applied for your TMAN and it is approved
- You have all the relevant information that is required within TOMS
- Road space has been granted by permitting process via Street Manager.
- The required lead times are viable, i.e. you need 8 weeks for a section 14.1 order (see above for guidance).

STOT cannot process your application until all of the above conditions have been met otherwise requests submitted will be rejected. Please do not request a GLA number in TOMS until it is certain to go ahead.

All requests for TRO numbers should be made directly in TOMS. You will require Londonworks access for this function you will need to send an email to Londonworks@tfl.gov.uk and request "Applicant Access" for TOMS. General requests for TRO training in TOMS should be made by contacting Sufi Waheed SufiyanWaheed@tfl.gov.uk.

5.6 PAYMENT AND INVOICING

The Traffic Orders Team will generally charge for TROs on a 4 weekly basis. You will be required to submit a blanket Purchase Order to cover your TRO sites. STOT will call-off payment once the TRO is completed. An invoice will be sent every 4 weeks for payment by internal.

EVID Contractors will need to register with TfL in order for payments to be made via BACS (see Appendix C). STOT will process the application on the Contractor's behalf, when the information requested at Appendix B is received. The cost for Traffic Orders is outlined in the TRO Costs document set out in Appendix C. The cost is based on a single application and therefore, for any additional sites within a borough will incur an additional £100 advertising cost.

TRO costs will increase on an annual basis in line with inflation.

5.7 HS2 INFORMATION

All temporary traffic orders in the City of London, City of Westminster, the Royal Borough of Kensington and Chelsea and the London Boroughs of Islington, Tower Hamlets, Southwark, Lambeth, Camden, Hammersmith and Fulham, Ealing, Brent and Hillingdon require agreement with High Speed 2 legislation. Please be aware that the Secretary of State can veto any proposed Order that he or she believes will be a negative impact on HS2 works. If this happens your works cannot proceed. If you have already consulted HS2 you will need to supply evidence of the consultation with your Traffic Order application or ask STOT to comply on your behalf.

Appendix A

Barnet	Agatha Obiekwe	AgathaObiekwe@tfl.gov.uk
Barking & Dagenham	Rohan Chandra	ChandraR@tfl.gov.uk
Bexley	Bryan Spaans	BryanSpaans@tfl.gov.uk
Brent	Agatha Obiekwe	AgathaObiekwe@tfl.gov.uk
Bromley	Bryan Spaans	BryanSpaans@tfl.gov.uk
Camden	Olu Mosuro	OluMosuro@tfl.gov.uk
City of London	Sufi Waheed	SufiyanWaheed@tfl.gov.uk
Croydon	Sufi Waheed	SufiyanWaheed@tfl.gov.uk
Ealing	Agatha Obiekwe	AgathaObiekwe@tfl.gov.uk
Enfield	Olu Mosuro	OluMosuro@tfl.gov.uk
Greenwich	Bryan Spaans	BryanSpaans@tfl.gov.uk
Hackney	Olu Mosuro	OluMosuro@tfl.gov.uk
Hammersmith and Fulham	Lase Laleye	LaseLaleye@tfl.gov.uk
Haringey	Olu Mosuro	OluMosuro@tfl.gov.uk
Harrow	Agatha Obiekwe	AgathaObiekwe@tfl.gov.uk
Havering	Rohan Chandra	ChandraR@tfl.gov.uk
Hillingdon	Agatha Obiekwe	AgathaObiekwe@tfl.gov.uk
Hounslow	Lase Laleye	LaseLaleye@tfl.gov.uk
Islington	Olu Mosuro	OluMosuro@tfl.gov.uk
Kensington and Chelsea	Lase Laleye	LaseLaleye@tfl.gov.uk
Kingston-upon-Thames	Sufi Waheed	SufiyanWaheed@tfl.gov.uk
Lambeth	Sufi Waheed	SufiyanWaheed@tfl.gov.uk
Lewisham	Bryan Spaans	BryanSpaans@tfl.gov.uk
Merton	Sufi Waheed	SufiyanWaheed@tfl.gov.uk
Newham	Rohan Chandra	ChandraR@tfl.gov.uk
Redbridge	Rohan Chandra	ChandraR@tfl.gov.uk
Richmond	Lase Laleye	LaseLaleye@tfl.gov.uk
Southwark	Bryan Spaans	BryanSpaans@tfl.gov.uk
Sutton	Sufi Waheed	SufiyanWaheed@tfl.gov.uk
Tower Hamlets	Rohan Chandra	ChandraR@tfl.gov.uk
Waltham Forest	Rohan Chandra	ChandraR@tfl.gov.uk
Wandsworth	Lase Laleye	LaseLaleye@tfl.gov.uk
Westminster	Bryan Spaans	BryanSpaans@tfl.gov.uk

Email Address:
TrafficOrderSection@tfl.gov.uk

Network Management Directorate

Name		Job Title	Auto	Email
Pauline	**Anderson**	Traffic Orders Manager	81121	Pauline.Anderson@TfL.gov.uk
Gerald (Gerry)	**Kelly**	Senior Traffic Orders Officer	81296	Gerald.Kelly@TfL.gov.uk
Bryan	**Spaans**	Senior Traffic Orders Officer	81291	BryanSpaans@tfl.gov.uk
Rohan	**Chandra**	Senior Traffic Orders Officer	81332	ChandraR@tfl.gov.uk
Lase	**Lalege**	Senior Traffic Orders Officer	81238	LaseLaleye@tfl.gov.uk
Sufiyan (Sufi)	**Waheed**	Senior Traffic Orders Officer	84367	Sufiyanwaheed@tfl.gov.uk
Agatha	**Obiekwe**	Senior Traffic Orders Officer	83177	AgathaObiekwe@tfl.gov.uk
Olu	**Mosuro**	Senior Traffic Orders Officer	85712	OluMosuro@tfl.gov.uk

Appendix B

Company Name :

Trading Name:

Registered address:

Trading / billing address:

Company registration no:

Accounts payable name(s):

Telephone number(s):

Generic AP email address for invoice to be sent to:

Alternative email address for key contact:

Please provide detailed description of your request:

Appendix C

Section 6 Permanent Traffic Regulation Order	
Administration: Assessment of Application, processing Order compliance with statutory regulations including formal consents, obligatory notifications to all parties of the event and system input.	£1000.00
Advertising: Publication of Notices (Media, Street and Web). Liaison and notifications to Contractors and Media Groups.	£2050.00
TOTAL	£3050.00

Section 14(1) Temporary Traffic Regulation Order*	
Administration: Assessment of Application, processing Order compliance with statutory regulations, obligatory notifications to all parties for delivery of the works and system input.	£1450.00
Advertising: Publication of Notices (Media, Street and Web). Liaison and notifications to Contractors and Media Groups.	£1450.00
TOTAL	£2900.00

Section 14(1) Temporary Traffic Regulation Order & Temporary Suspension Request	
Administration: Assessment of Application, processing Order compliance with statutory regulations, obligatory notifications to all parties for delivery of the works and system input. Draft, and issue notice, liaising with Contractor directly.	£1450.00
Advertising: Publication of Notices (Media, Street and Web). Liaison and notifications to Contractors and Media Groups.	£1450.00
Signage: Instruct contractor to implement suspension, including notification to all parties, erection and removal of notice, checking site compliance and statutory compliance.	£400.00
TOTAL	£3300.00

Section 14(2)(a) Temporary Traffic Regulation Notice*	
Administration: Assessment of Application, processing Order compliance with statutory regulations, obligatory notifications to all parties for delivery of the works and system input. Draft, and issue notice, liaising with Contractor directly.	£1500.00
TOTAL	£1500.00

Section 14(2)-14(1)Temporary Traffic Regulation Notice and Order	
Administration: Assessment of Application, processing Order compliance with statutory regulations, obligatory notifications to all parties for delivery of the works and system input. Draft, and issue notice, liaising with Contractor directly.	£1250.00
Advertising: Publication of Notices (Media, Street and Web). Liaison and notifications to Contractors and Media Groups.	£1450.00
Signage: Instruct contractor to implement suspension, including notification to all parties, erection and removal of notice, checking site compliance and statutory compliance.	£400.00
TOTAL	£3100.00

Section 14(2)(b) Temporary Traffic Regulation Notice & Temporary Suspension Request	
Administration: Assessment of Application, processing Order compliance with statutory regulations, obligatory notifications to all parties for delivery of the works and system input. Draft, and issue notice, liaising with Contractor directly.	£1500.00
Signage: Instruct contractor to implement suspension, including notification to all parties, erection and removal of notice, checking site compliance and statutory compliance.	£400.00
TOTAL	£1900.00

Section 15(2) Temporary Traffic Regulation Order & Temporary Suspension Request	
Administration: Stage 1 Implementation - Assessment of Application, processing Order compliance with statutory regulations, obligatory notifications to all parties for delivery of the works and system input.	£1700.00
Stage 2 Revocation - Receipt of application that works have now been completed. Check notification and process application. Notify all parties and remove TRO from all systems. Instruct publication insert and removal from site.	£1700.00
Advertising: Stage 1 - Publication of Notices (Media and Web) i.e. notices of Intent and Making	£1450.00
Stage 2 - second advertising process as Stage 1 for the revocation of initial stage. Liaison and notifications to Contractors and Media Groups.	£850.00
TOTAL	£5700.00

Revocation of Traffic Regulation Order/Notice Request	
Administration: Assessment of Application, processing Order compliance with statutory regulations, obligatory notifications to all parties for delivery of the works and system input. Draft, and issue notice, liaising with Contractor directly.	£1700.00
Signage: Instruct contractor to implement suspension, including notification to all parties, erection and removal of notice, checking site compliance and statutory compliance.	£600.00
TOTAL	£2300.00

"Golden Rules" for producing Traffic Order plans

Following the nine "Golden Rules" can help avoid any delays to your application

1. Include scales and dimensions

Traffic Orders need to be accurate to within ½ metre. Including scales and dimensions in your plans enables us to reach this precision, and gives us confidence that we have accurately understood your requirements.

2. Include compass points

Knowing which way is North helps us to orientate your plan.

3. Include street names and building numbers

Including all street names and building numbers speeds up our work and provides context for any stakeholders who may view the plans.

4. Show existing and proposed layouts separately

The clearest way to highlight the changes you wish to make is to show the proposed and existing layouts side-by-side on separate maps. Superimposing all the details onto a single map increases the risk of us missing something!

5. Include a detailed list of changes

Another way to avoid anything being overlooked is to include a list of the changes you would like to make. This is especially important for complex schemes.

6. Measure locations from fixed building lines

Traffic Orders can remain in force for decades, so avoid using temporary landmarks, like trees or road markings, as reference points. Fixed building lines or easily identifiable property boundaries are ideal.

7. Add a splash of colour

For example, we love it when single-red or double-red lines appear on the plan in red, rather than black-and-white. This enables us to understand your plan at a glance.

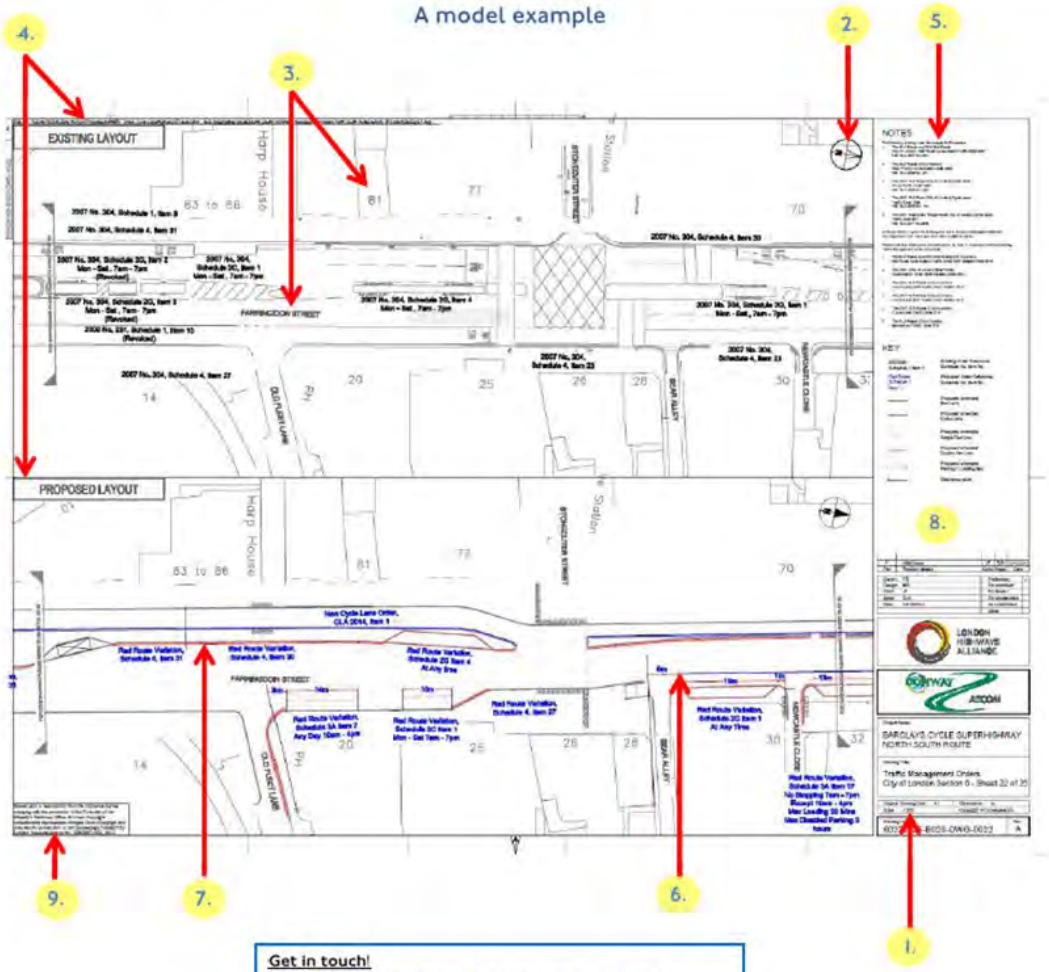
8. Make it look professional

We might need to use your plans for consultation. To make the best impression on your stakeholders, try not to draw or annotate your plans by hand.

9. Use up-to-date maps

We've been caught-out by this more than once!

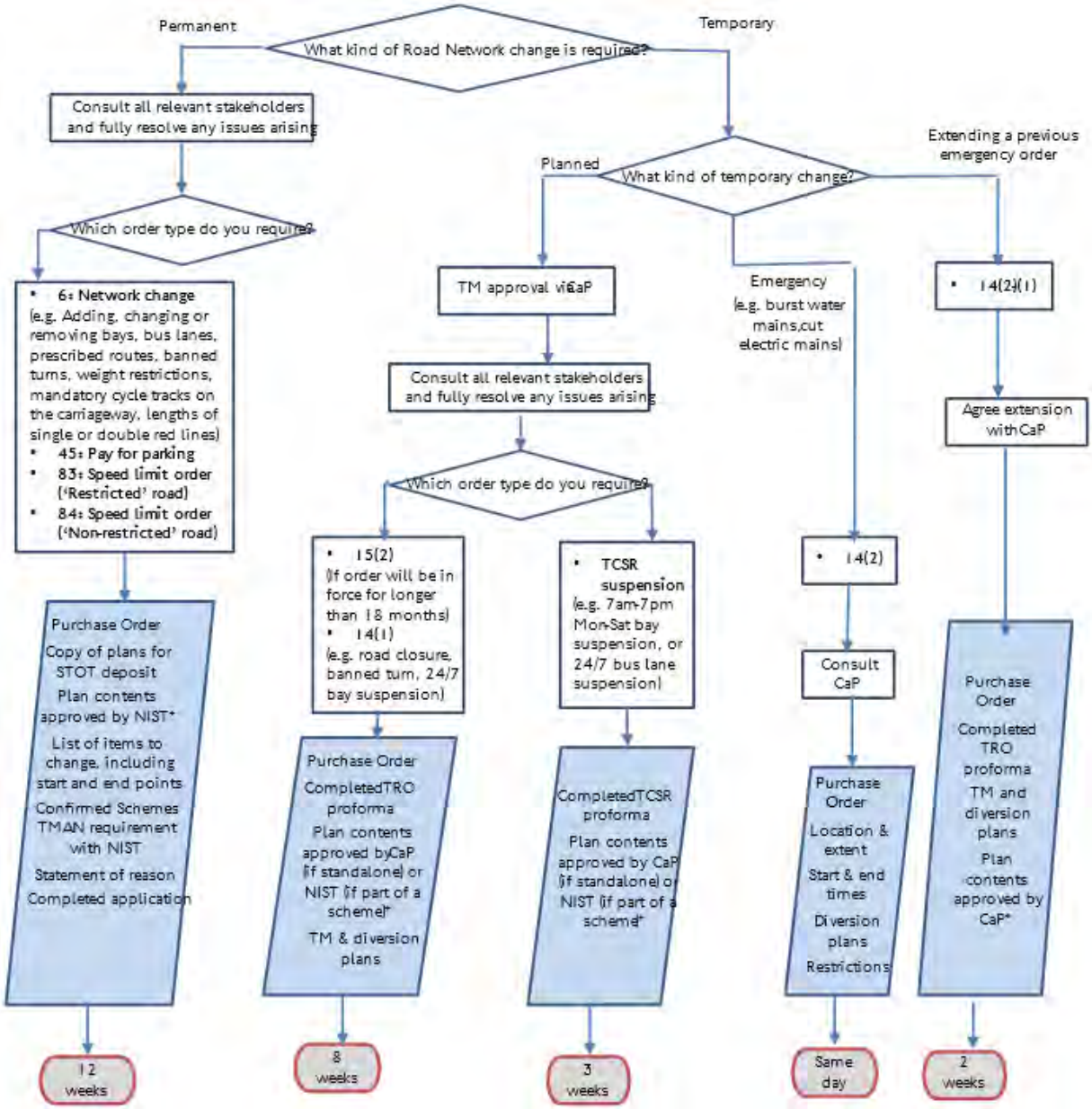
A model example



Get in touch!
Email: TrafficOrderSection@streetmanagement.org.uk
Phone: 83177 / 81238/ 64837 / 80932 / 81332 / 81291 / 81296 / 81121
Face-to-face: Come and find us at Palestra, 3R3!

Appendix D: "Golden Rules" for producing Traffic Order plans

Appendix E


What kind of Road Network change is required?
Permanent
Temporary
Consult all relevant stakeholders and fully resolve any issues arising
Which order type do you require?
• 6: Network change (e.g. Adding, changing or removing bays, bus lanes, prescribed routes, banned turns, weight restrictions, mandatory cycle tracks on the carriageway, lengths of single or double red lines)
• 45: Pay for parking
• 83: Speed limit order ('Restricted' road)
• 84: Speed limit order ('Non-restricted' road)
Purchase Order
Copy of plans for STOT deposit
Plan contents approved by NIST*
List of items to change, including start and end points
Confirmed Schemes TMAN requirement with NIST
Statement of reason
Completed application
12 weeks
What kind of temporary change?
Planned
Emergency (e.g. burst water mains,cut electric mains)
Extending a previous emergency order
TM approval via CaP
Consult all relevant stakeholders and fully resolve any issues arising
Which order type do you require?
• 15(2) (If order will be in force for longer than 18 months)
• 14(1) (e.g. road closure, banned turn, 24/7 bay suspension)
Purchase Order
CompletedTRO proforma
Plan contents approved byCaP (if standalone) or NIST (if part of a scheme)*
TM & diversion plans
8 weeks
• TCSR suspension (e.g. 7am-7pm Mon-Sat bay suspension, or 24/7 bus lane suspension)
CompletedTCSR proforma
Plan contents approved by CaP (if standalone) or NIST (if part of a scheme)*
3 weeks
• 14(2)
Consult CaP
Purchase Order
Location & extent
Start & end times
Diversion plans
Restrictions
Same day
• 14(2)(1)
Agree extension withCaP
Purchase Order
Completed TRO proforma
TM and diversion plans
Plan contents approved by CaP*
2 weeks

Transport for London

Invitation to Quote

Electric Vehicle Infrastructure Delivery (EVID)
Tranche 2, Batch 1

Volume 2

Appendix R

Safer Provisions For Pedestrians At Roadworks

COMMERCIAL IN CONFIDENCE

TfL Restricted

Safer Provisions for Pedestrians at Roadworks

A Risk Prioritisation Framework



Purpose

The objective of this document is to help improve TfL's safety scorecard metrics that exist to keep people safe where roadworks is being carried out on our road network. The aim is to specifically address a known problem area where a disproportionate number of high-risk failures have been recorded where pedestrian provisions have been found to be inadequate. This guidance is primarily aimed at those who are responsible for either designing or assessing works traffic management proposals.

Background:

In January 2019 TfL launched its Temporary Traffic Management Handbook (TTMH) to help enhance the safety of road users when navigating around roadworks, particularly those that are more vulnerable. The TTMH highlights that 78 per cent of people killed or seriously injured on the TLRN in the vicinity of roadworks were those that walk or cycle. Despite work promoters adopting this additional guidance, which supplements national standards (such as the Safety Code and Chapter 8), high-risk failures for inadequate pedestrian management is still trending upwards, with some utility companies prosecuted for being found in breach of these standards. To statistically qualify the matter further, over the 12 month period from January 2021, the high-risk safety inspection failure rate (category A) for non-compliant pedestrian provisions on the TLRN stood at 32%, which translates to a raw number of 261 high-risk failures within a single year. The government have also recognised the risks pedestrians are exposed to on the highway by recently updating the Highway Code to give pedestrians the highest road user priority and bear the least responsibility for other road users.

The Problem:

There is a misconception by some that picking any traffic management (TM) arrangement from the national standards is a satisfactory solution, without taking into consideration the risks associated with how a strategic road network operates or the surrounding characteristics of the highway where the works are proposed. That is not a defendable approach and unlikely to withstand legal scrutiny, unless it can be evidenced that all other options have been considered and justification provided as to why they were not viable.

Implementing lengthy pedestrian diversions is a common scenario where the incorrect choice of temporary traffic management is made, particularly at busy junctions, where 76 per cent of all collisions occur. In reality pedestrian diversions can often be ignored or misunderstood, with some people instinctively following their natural desire lines and unwittingly putting themselves in danger by walking unprotected in live traffic. They are also extremely difficult to understand by people that are either disabled (particularly those with visual impairments), older or are accompanied by children. Similarly, designing traffic management without undertaking a pre-works site inspection to understand how the street is used can be equally detrimental, particularly if there are high numbers of more vulnerable pedestrians because there are nearby hospitals, care homes or schools; or there are heavy footfall arears due to the vicinity of public transport services. While the works are in progress the works contractor should be checking throughout the day that the traffic management arrangements in place are compliant and appropriate for the way the street is being used.

The Problem continued…

Every works and its locality are unique and must therefore always be subject to a site-specific risk assessment, which will help determine what the safest possible TM solution should be implemented. This is one of the key principles that features across all TM standards, and it is vital that TM designers observe this responsibly.

Where TfL's Roadworks Enforcement Inspectors do observe unsafe road user behaviour at sites and notice multiple instances where pedestrians appear confused that would not normally occur at the same location under non-works conditions, it is likely they will deem the traffic management to be ineffective and are duty bound to record a non-compliant inspection to identify the presence of inadequate provisions that are compromising the ability to safeguard pedestrian journeys.



The general principles stated within national TM standards make it explicit that:

- Works should cause minimum inconvenience to road users;
- Pay particular attention to the needs of disabled people and other vulnerable groups such as elderly people, children and those with push chairs.
- Potential conflict between road users should be minimised;
- The chosen method of working must not increase risk to road users;
- Exposure to unsafe, or otherwise unacceptable, conditions is minimised, if not eliminated. For road users this can be taken as the level of safety and road user comprehension expected for the same road in non-works conditions; and
- Work promoters have a responsibility to ensure the safety of those passing near or through works, including protecting pedestrians from traffic

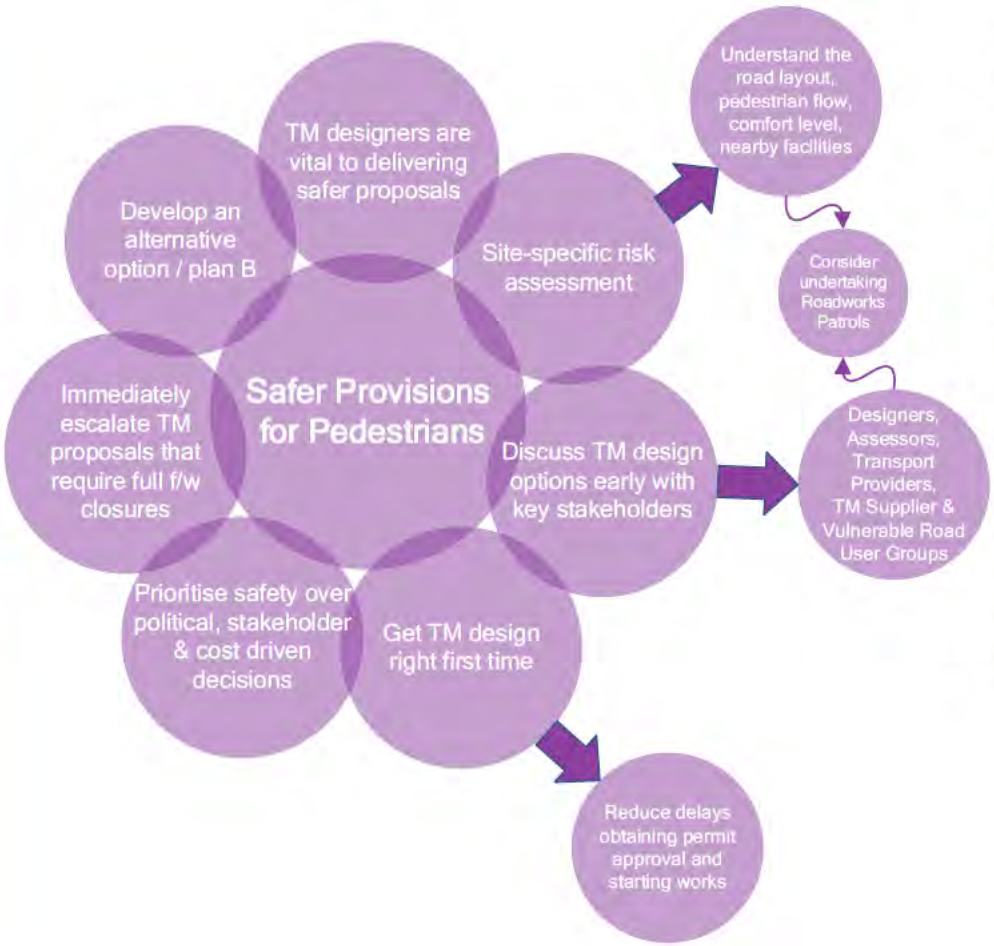
It is therefore unacceptable to produce TM proposals, such as lengthy and unintuitive diversions, that ignore the prospect of not being followed and thus render the TM recommendation unfit for purpose. The mindset of believing that selecting the easiest solution (but not always the safest) from the national standards does not in any way absolve individuals or organisations of liability just because it exists as an arrangement in these documents.

Every works and its locality are unique and must therefore always be subject to a site-specific risk assessment, which will help determine what the safest possible TM solution should be implemented. This is one of the key principles that features across all TM standards, and it is vital that TM designers observe this responsibly.

Safer Provisions for Pedestrians at Roadworks

A Risk Prioritisation Framework

Proposed Improvements

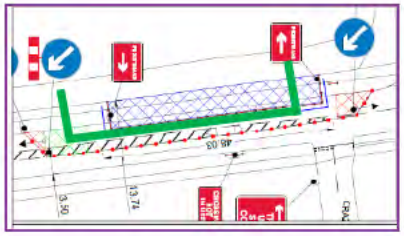


To achieve the optimum TM solution it is important to take a collaborative approach by engaging with the key stakeholders as early as possible in the design process to ensure safety is prioritised throughout – Roadworks Patrols (as described in section 10.12 of the TTMH) are a useful way of achieving this. The ven-diagram highlights some of the important element's TM designers should consider when delivering safer TM provisions for pedestrians.

As stated above, there have been several cases where the TM selection for several sites has been found to be inappropriate for the safe passage of pedestrians. To help support TM designers and assessors agree the most appropriate traffic arrangement, the following priority framework has been developed.

Hazard	Risk and Effect	Control Measures and Further Considerations

Reduced footway width	• Increased pedestrian congestion can lead to pedestrians using the carriageway and subsequently interfere with other modes of transports
	• Sight lines may become obscured
	• Exacerbation of existing obstructions such as street furniture
	 
	 
	Maintaining route on existing footpaths preserves road user comprehension and causes minimum inconvenience
		• Statutory minimum widths should be sufficient at most locations. Where pedestrian congestion is known to exist prior to works it may be necessary to:
		  ○ avoid works during peak hours
		  ○ reduce the length of footway sites
		  ○ introduce passing points or wheelchair waiting areas where a 2-metre wide clearance cannot be provided
		  ○ place continuous guarding along kerbside to prevent errant pedestrian movements
		• Pedestrian desire lines must be met as closely as possible, with existing pedestrian crossing facilities included within access plans where it is practical
		• Works may need to be phased to ensure that safety critical sight lines at pedestrian crossings are not compromised
		• Temporary routes should be delineated by continuous pedestrian barriers that can be closely followed by those with visual impairments and other vulnerabilities

Temporary pedestrian route in adjacent highway	• Transitioning from footway to carriageway • Maintaining access to properties/frontages 	• Statutory requirement for kerb ramps that adhere to DfT Inclusive Mobility guidance by ensuring that moving pedestrians from footway to carriageway is accessible for all users • Arrangements should be made to provide direct continuous access wherever possible, with statutory minimum widths unimpeded by projecting barrier feet. • Bespoke access arrangements should be agreed in exceptional circumstances    Re-providing route in adjacent highway maintains desire lines. Careful consideration should be given to situations where this option disproportionately impacts the flow of bus services (see below).

Hazard	Risk and Effect	Control Measures and Further Considerations
Parallel alternative pedestrian route on opposite footway	• Temporary routes that deviate significantly from existing ones are often misunderstood and cause pedestrians to enter the live carriageway to pass sites • Introducing waiting times increases crowding which can obscure pedestrian signs informing users of the temporary route, resulting in pedestrians entering the live carriageway • Access to properties within closed sections of footways can cause confusion resulting in unsafe pedestrian movements	• Ensuring that approaching pedestrians can see the extent of the footway closure and the alternative route increases the likelihood of the route being understood and followed. This can be achieved by keeping the routes short. Having dedicated site personnel at closure/crossing points to assist pedestrians, especially those requiring assistance or reassurance, can increase comprehension, but may not be practical in very busy areas where demand is high • Vulnerable pedestrians are at increased risk when crossing strategic roads with high traffic volumes, which can only be reduced by ensuring controlled temporary crossing facilities are provided – these must include tactile features to assist those with visual impairments • Use of existing controlled crossing points may be preferable when their position allows minimal departure from existing desire lines. However, their use should be avoided if it requires routes that introduce excessive and unintuitive pedestrian movements with complicated access arrangements – making "hard" footway closures impractical or prone to inference. In these instances, portable pedestrian crossing facilities should be considered.  Pedestrian routes with significant deviation are often misunderstood and cause pedestrians to enter the carriageway
Indirect alternative route	• Pedestrian re-routing in opposition to usual routes/desire lines are rarely understood and frequently result in unsafe pedestrian movements • Vulnerable pedestrians (especially those with visual impairments) are more likely to be disadvantaged by alternative and unintuitive routes with multiple crossing points	• This type of pedestrian management should generally be avoided by adopting the above lower risk methods instead • Only consider for exceptional circumstances where the work activity area cannot practically be reduced, such as for mobile crane operations. The timing and duration of the activity should be chosen to ensure minimal impact to road users • Dedicated operatives should be placed throughout the alternative route to: o mitigate the risk of pedestrians misunderstanding any forced change of direction; and o ensure that vulnerable pedestrians can be fully escorted through the route  Lengthy pedestrian diversion routes are often ignored with road users electing instead to follow natural desire lines

Hazard	Risk and Effect	Control Measures and Further Considerations

Off public highway routes	• Pedestrian re-routing through adjoining private land or public rights of way can increase the likelihood of pedestrians encountering:
	  ○ certain types of crime, disorder or antisocial behaviour (particularly towards women) that would ordinarily be avoided if the public footway was available
	  ○ trip hazards and obstructions
	  ○ Unnegotiable routes that contain steps, high gradients or inadequate tactile features, which are problematic for some disabled pedestrians
		• Temporary pedestrian provisions should feel safe and avoid creating potential ambush points or concealed areas that isolate pedestrians from remaining highway users. Introducing temporary lighting or the permanent presence of site staff along temporary routes may address these issues in limited circumstances, but views from the local Police service should always be sought, as well as input from disabled, older and women road user groups.
		• It may be possible to survey the condition of alternative routes to ensure they are maintained to a satisfactory standard that is equal or superior to public highway routes. However, the position with liability on private land should be understood as it is unlikely that powers relating to public highways can be exercised in these circumstances and should therefore be avoided.
		• Routes accessible for those with disabilities must always be provided. Sometimes it may be possible to provide more than one temporary pedestrian route, but the primary route must be fully accessible and inclusive to prevent disadvantaging any groups of people using it in comparison to other temporary routes i.e. the primary route should not be excessive in length. It should also be ensured that the primary route is not easily confused with closed off routes.
		   
		Diverting pedestrians across private land or forecourts is not suggested unless liability for public safety has been established and the route has been satisfactorily maintained

Other Considerations

Works Sequencing:

Phase the construction work to maintain minimum footway widths by reducing the working area. For example: half width reconstruction

Works Timing:

Undertake works activity when footfall is at an acceptably low level – pulling in TM during peak travelling periods. For example:

- At off-peak periods, overnight or at weekends; or
- Temporarily plating over excavations or temporarily reinstating

Maintain Existing Cycling Provisions

Existing provisions for cyclists should be re-provided, ideally by means of a dedicated temporary cycle lane, or where that is not possible consider narrowing lanes as advised in the TTMH.

Where motorised running lane widths are compromised and it is necessary to divert motorised vehicular traffic, consideration should be given to maintaining cyclists access.

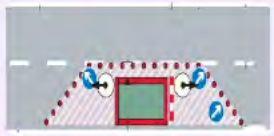


Maintain Bus Services

Maintaining existing bus services and associated infrastructure such as bus stops should be prioritised wherever possible in favour of lengthy diversions or relocating bus stops – particularly where ridership is high. Wherever running lane widths are compromised consideration should be given to diverting regular motorised vehicular traffic in favour of maintaining cycle and bus provisions.

For example:

- Implementing extraordinary traffic control measures to facilitate continued bus provisions, such as:
  - Traffic control by portable activated traffic signals
  - Traffic control by stop/go boards
  - Traffic control by priority signs
- Implementing extraordinary traffic control measures to facilitate one-way traffic for the direction with the highest level of bus flow, while placing the opposing directional traffic on diversion





Justification for Selected Traffic Management Arrangement

Traffic management designers are encouraged to complete this template and submit it to TfL Traffic Management Assessors with their traffic management proposals to demonstrate they have carefully considered each option in risk priority order before determining the most suitable traffic management solution

Title of Scheme Works:	[INSERT HERE]	Site Location:	[INSERT HERE]
Pedestrians – Average Daily Flow:	[INSERT HERE]	Cyclists – Average Daily Flow:	[INSERT HERE]
Buses – Hourly Count:	[INSERT HERE]	All Vehicle – Average Daily Flow:	[INSERT HERE]
Pedestrian Data 	Cyclist Data – Coming soon	Bus Data 	All Vehicle Data 

Pedestrian, bus and all vehicle daily flows are currently available from TfL's Playbook, with cyclist data following soon. Please contact Playbook@tfl.gov.uk for access or requests for mapping data files.

Risk Description (select one or more)	Achievable? ☑ = STOP ☐ = Next Priority ↓	Justification (explain why preceding solutions are not suitable, together with a statement to validate the chosen solution)
Maintain minimum width for pedestrians on existing footway		
Re-provide minimum width for pedestrians in adjacent highway		
Provide alternative parallel route on opposite footway		
Provide an indirect alternative route		
Off public highway routes		

Transport for London

Invitation to Quote

Electric Vehicle Infrastructure Delivery (EVID)
Tranche 2, Batch 1

Volume 2

Appendix S

Carbon & Resource Plan

COMMERCIAL IN CONFIDENCE

TfL Restricted

Carbon and Resource Plan (CRP)

Directorate	Investment Planning
Programme	Electric Vehicle Infrastructure Delivery
Reference	ST-PJ003C
Pathway Stage	Option Selection – Stage Gate 2b

Responsible (1)	Project Engineer	Lixi Pan
	 Signature	Date 16/05/2024

Accountable	Project Manager	Abrahim Ahmed
	 Signature	Date 21/05/2024

Reviewed by (2)	Project Engineer	Kristy Yiu
	Signature 	Date 16 May 2024

Product History	**Version**	**Date**	**Author**	**Summary of changes**
	1.0	16/05/24	Lixi Pan	First issue

(1) The person(s) responsible for the design should produce this document. All designers should be consulted and all project stakeholders aware of any actions to ensure Carbon is considered in decision making.
(2) If Designer signs as Responsible, then Project Engineer signs Reviewed by

Product Context

Purpose	The purpose of the Carbon and Resource Plan is to encourage and facilitate the reduction of whole life carbon emissions, energy consumption and waste production through the application of the carbon, energy, and waste reduction hierarchies.

Applicability	The Carbon and Resource Plan must be produced for all projects/programmes impacting assets or creating new assets. This product is normally created at project level, but if appropriate and agreed with the SHE Sustainability and Corporate Environment team, it may be produced for a group of projects or programme.

	Role	Detail
Consult Consider these roles when developing this document.	Sponsor	To be involved in carbon and resource workshops so that carbon, energy and waste are considered and captured in the development of the business case
	Operations Representative	To propose savings initiates and ensure those proposed by others consider the benefits and disbenefits of each option from their perspective.
	Maintenance Representative	To propose savings initiates and ensure those proposed by others consider the benefits and disbenefits of each option from their perspective.
	Commercial Lead	To propose savings initiates and ensure those proposed by others consider the benefits and disbenefits of each option from their perspective.
	Subject Matter Experts	To propose savings initiates and ensure those proposed by others consider the benefits and disbenefits of each option from their perspective.
	Construction Lead / Manager	To propose savings initiates and ensure those proposed by others consider the benefits and disbenefits of each option from their perspective.
	SHE Corporate Environment	Subject Matter Expert for carbon and the environment who may audit this document. Will also propose savings initiatives and ensure those proposed by others consider the benefits and disbenefits of each option from their perspective.

TfL RESTRICTED

Characterisation Table	Category Level			
	Simple	Standard	Significant	Major
All sections	Required	Required	Required	Required

General Notes:

- The whole life carbon management process for projects can be found on this page including relevant links to each lifecycle stage specific process and guidance.

If you have any queries, feedback, or improvement suggestions about this product, then please contact tflpathway@tfl.gov.uk.



Table of Contents

Distinguishing elements of the Carbon Management Process 7

Introduction to completing the Carbon and Resource Plan: the Carbon, Energy and Waste Reduction Hierarchies 8

Step 1: Carbon and Resource Workshops 9

Step 2: Carbon and Resource Opportunities Tracker 12

Step 3: Carbon and Resource Trackers 14

Distinguishing elements of the Carbon Management Process

	Carbon and Resource Plan	Whole Life Carbon Model	Carbon Management Plan
Applicability	All projects impacting existing assets and installing new assets.	All projects impacting existing assets and installing new assets.	Schemes applying to DfT for funding.
Responsible	Project Engineer* *The person(s) responsible for the overall design should produce this document. All designers should be consulted and all project stakeholders aware of any actions to ensure Carbon is considered in all decision making.	Project Engineer	Project Manager
Purpose of deliverable	Support the identification of carbon, energy and waste reduction opportunities and their implementation to enable low carbon, energy, and waste outcomes: • Provides guidance for Carbon and Resource Workshops and supports capture of discussions • Tracks Carbon, Energy and Waste reduction opportunities and their outcomes	Quantitative assessment of whole life carbon.	Integrated or separate component of a schemes Management Case that details the plan for Carbon Management on a project, including assumptions, boundaries and scope of Whole Life Carbon assessment and modelling; RACI for enacting Carbon Management; monitoring and reporting plans, and Whole Life Carbon reporting.

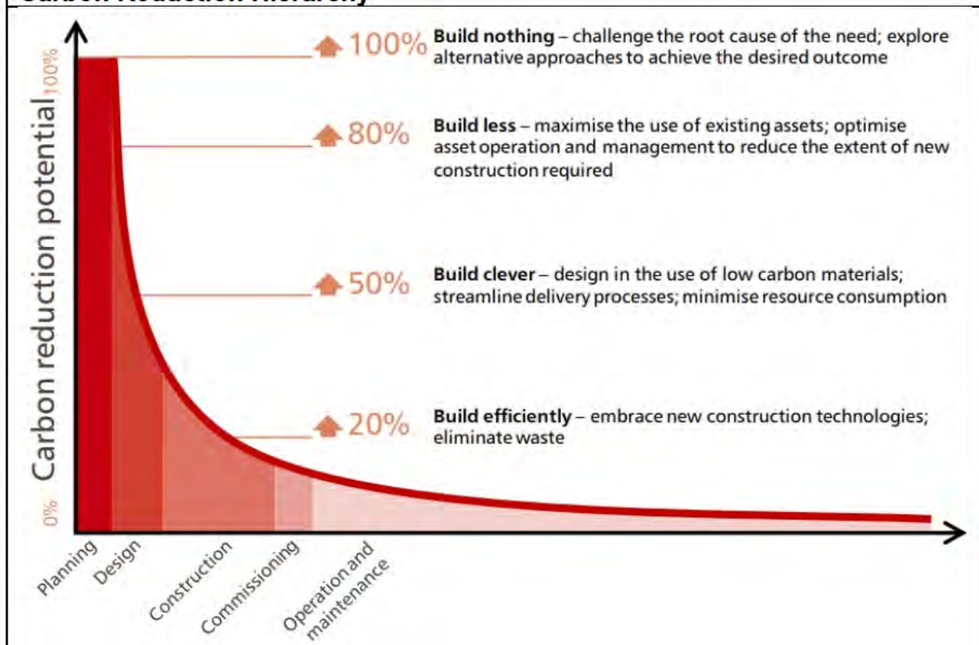
Creation and Updates	The CRP is Created at Option Selection and reviewed and updated at each Pathway Stage.	The Pathway Stage at which to begin modelling is defined in the Environmental Evaluation according to characterisation:
		• Major/Significant – Outcome Definition
		  ○ Quantitative modelling at longlist and shortlist
		• Standard – Option Selection
		  ○ Qualitative assessment at longlist
		  ○ Quantitative model at shortlist
		• Simple – Concept Design
		
		The first quantitative Whole Life Carbon model produced for project is the Carbon Baseline. Updates or replacement of the Carbon Baseline must be managed by Change Control and only occur under specific circumstances.
		
		Throughout the project, Live/Realised Carbon Models continuously track the latest design of a project. These may be produced as "updates" of previous Carbon Models or created new depending on the changes to the underlying assumptions and data used to create the Models.
			Multiple per project (one report or report revision per stage). A carbon management plan template is held within business case guidance.

TfL RESTRICTED

Introduction to completing the Carbon and Resource Plan: the Carbon, Energy and Waste Reduction Hierarchies

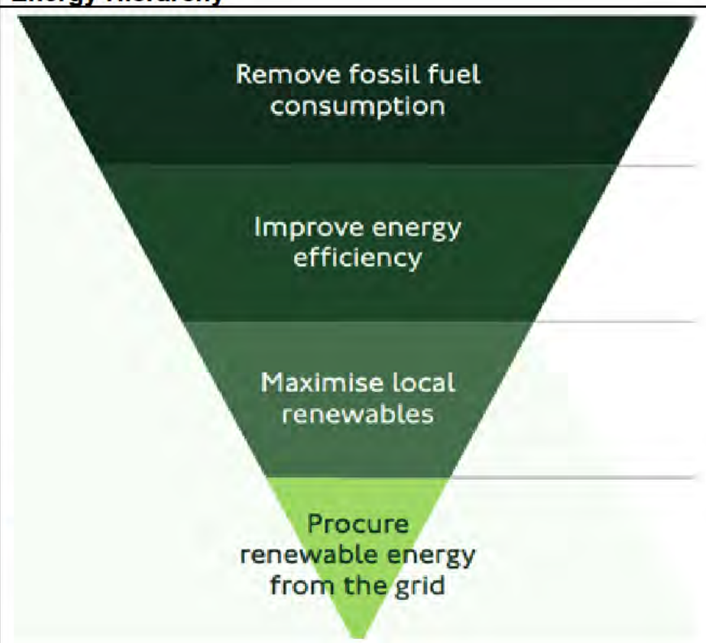
Transport for London must support London's ambitions to become a zero-carbon and zero-waste city. To reduce the Carbon, Energy and Waste associated with Transport for London's activities, projects impacting existing assets or installing new assets must complete the Carbon and Resource Plan (CRP). The CRP supports London's ambitions by requiring projects to identify and implement opportunities aligned with the Carbon, Energy and Waste Reduction Hierarchies:

Carbon Reduction Hierarchy



Source: Infrastructure Carbon Review (2013)

Energy Hierarchy



Note: procuring renewables should not be considered at a project/programme level.

Waste Hierarchy



The CRP provides a framework for projects to use the hierarchies by:

- providing guidance for using the hierarchies in "Carbon and Resource Workshops" to identify reduction opportunities and supports capture of these discussions
- tracking identified opportunities and their outcomes

Step 1: Carbon and Resource Workshops

- At the start of each Pathway Stage, the Designer must lead a Carbon and Resource Workshop with the project team and stakeholders to identify Carbon, Energy and Waste reduction opportunities for the project. Attendees should include the Designer, Project Manager, Engineers, Sponsor, SHE Business Partners, Construction Managers (where assigned), Maintenance or Operations representatives (where appropriate).
- The workshop may be structured by using the prompting questions below to explore opportunities for minimising carbon, energy and waste and discuss their validity. Where quantified information is available, resource and carbon Hotspots (Tables 2 and 5) should be explicitly considered. Projects may also use their cost and schedule Risk Registers to identify opportunities for cost reductions that also impacts carbon, energy, and waste.
- This section supports these workshops by:
  - Providing prompts for workshop discussion in line with the Carbon, Energy and Waste reduction hierarchies to spark conversation and ideas of opportunities in the categories of: Materials, Transport, Delivery, Maintenance & Replacement, Operational Energy, and End of Life
  - Providing space for projects to make notes during the workshops
- As projects develop their quantitative Whole Life Carbon Models, Energy models and Waste estimates (summarised in Tables 2-7), they should prioritise discussion of opportunities aimed at reducing the identified hotspots.
- Note: Words like 'build' in the table below can be easily swapped for 'deliver, manufacture, procure' to suit the needs of the project.

For further guidance, resources, and examples of reduction opportunities, please review Part 2 of the Carbon Management Training Suite.

	Option Selection	Concept Design	Detailed Design	Delivery
Date of Workshop	13/05/2024			
Workshop led by (Designer and Organisation Name):	Lixi Pan (TfL Engineering)			

Materials & End of Life	Build Nothing	What can be descoped? How can the functionality be achieved without buying and/or constructing a new asset? What alternatives could achieve the same outcomes and benefits?
	Build Less	How can existing assets and systems be retrofitted, modified, or repurposed to achieve the project outcomes? How can existing communication systems be used? How can the life of existing assets be maximised? How can the design be made smaller? How can the quantities of materials be minimised? How can the reuse of site material be maximised (e.g., from demolition and site clearance)? Can elements of the existing infrastructure or materials be re-used (rather than building from new)?
	Build Clever	Can off-site construction be used? Can modular construction be used? Are nature-based solution possible? Can less carbon intensive materials be used? (e.g., lower carbon cement and concrete alternatives, high-recycled content steel, higher recycled content) Can sustainable and regenerative material be used (e.g., timber)? Can materials be sourced locally? How can reusability at end of life be maximised? Can Circular Economy principles be considered in asset/material selection? What consideration has been given to sourcing materials for re-use from other TfL sites or other users? What steps have been taken to maximise the use of materials with recycled content? Can use be made of the sharing economy or using products as a service?
	Build Efficiently	How can rework be minimised? (Get It Right initiative) How can overordering be minimised?
Brainstorm	Build Less • Reusing existing material from site as much as is reasonably practicable, such as existing subgrade, kerbs and paving slabs. • Utilising existing signposts or lighting columns to mount new EV signs. Build Clever • Use fully recyclable bollards. Potentially bio-polymer bollards which have much less embodied carbon than steel or concrete bollards. • Use low carbon concrete where possible.	

TfL RESTRICTED

Transport	Transport Nothing	What is already on-site that can be used (e.g., plant, materials etc)?
	Transport Less	How can transport distances be minimised? How can the number of deliveries be minimised? Can materials be sourced from TfL stores or sites?
	Transport Clever	Is there a lower carbon transport option? Can lorries and vehicles be removed from the road?
	Transport Efficiently	How can vehicle loading be maximised? How can dead mileage be minimised?
Brainstorm	Transport Nothing • Use material available on site or locally sourced. Transport Less • Minimise deliveries to site. Transport Clever • Use electric vehicles to travel / deliver to site. • Use electrically powered plant during construction.	

Delivery	Deliver Nothing	What is already on-site that can be used (e.g., site electricity connection, site water supply)?
	Deliver Less	How can temporary works be minimised? How can the re-use of temporary works maximised? How can site electricity, fossil fuel and water consumption be minimised? How can time on site be minimised? Can more energy efficient plant be used?
	Deliver Clever	How can fossil fuel consumption be removed or minimised? How can plant use be minimised? Can renewable energy be used to power site cabins and facilities? Can SUDS be used on longer term construction sites? Can use be made of the sharing economy / using products as a service?
	Deliver Efficiently	How can rework be minimised? (Right First-Time initiative) How can plant utilisation be minimised?
Brainstorm	Deliver Nothing • Utilise readily available elements Deliver Less • Plan and coordinate the works efficiently before going on site. Deliver Clever • Use electrically powered plant during construction. Deliver Efficiently • Carry out GPR survey's, trial holes during the design stage to ensure re-work is reduced on site.	

Maintenance & Replacement	Use Nothing	How can the design life be maximised? Can maintenance be designed out?
	Use Less	How can maintenance be minimised? How can the durability of the design be maximised (to lessen the need for resources to be used for repairs in future)? How can durability be maximised?
	Use Clever	How can the future replacement of assets with lower carbon alternatives be supported? How can the resilience of other assets in the system be supported? How can the design be improved to make it resilient to extreme weather and climate change?
	Use Efficiently	How can asset condition be monitored?
Brainstorm	Use Clever • Incorporate the latest lower carbon alternatives in the designs. • Charger uses modular design. Module can be swapped out for replacement to minimise waste. Use Efficiently • Remote monitoring of EV charge point. • Liaise with TfL Asset Operations to include EV sites in their periodic site inspections.	

Operational Energy	Use Nothing	How can fossil fuel consumption be removed? Are passive options available? (e.g., skylights for maximising natural light, passive cooling, green/blue roof, sunshades)

TfL RESTRICTED

	Use Less	How can energy efficiency be maximised? How can energy consumption be minimised? Can more energy efficient products be chosen e.g., from the Energy Technology List?
	Use Clever	How can the use of local renewables be maximised on the asset or in the vicinity?[1] Can a heat pump be installed for heating?
	Use Efficiently	How can the utilisation of energy consuming assets be minimised? (e.g., motion sensors, heating/cooling programmes) Can out of hours consumption of energy be controlled/minimised?
Brainstorm	Use Clever • Source electricity from renewable electricity supplies for the EV charge points.	

End of life	Reduce	How can waste be minimised? How can the cut and fill balance be optimised to reduce the quantity of excavated material taken off site? Can less wasteful construction processes be used?
	Reuse	Are there identifiable projects or organisations that could make use of, or reuse, the project's waste? How can the reuse of site materials be maximised (e.g., from demolition and site clearance)? Can topsoil be reused on site or locally? How can the project aid disassembly for reuse?
	Repair	How can the project aid disassembly for repair?
	Recycle	How can the project aid disassembly for recycling? How can the recyclability of used materials be maximised? Can the recycling rates of transfer stations and/or recycling facilities be considered when selecting facilities to be used?
	Recover	After exhausting the above considerations, are there options for recovering energy or other useful returns from the waste?
	Dispose	How can the disposal of waste be minimised?
Brainstorm	Reduce • Maximising lifecycle of the asset beyond the end of the agreement where possible. Reuse • Reuse the charger for alternative usage post contract, such as EV hubs. Repair • Repair and replace with parts readily available to extend lifecycle of the asset. Recycle • Use recyclable material in order to recover and recycle at the end of cycle. Dispose • Dispose nonrecyclable and none re-coverable items in a responsible and environmentally friendly manner.	

[1] It is TfL strategic policy for all new build structures to install solar photovoltaic panels for electricity generation.

TfL RESTRICTED

Step 2: Carbon and Resource Opportunities Tracker

- Once opportunities are captured through the Carbon and Resource Workshops, they must be transferred to *Table 1 – Carbon and Resource Opportunities Tracker* for monitoring through to the end of the project. This process of transferring new opportunities will occur after each Pathway Stage Workshop.
- Projects may choose to add their CRP opportunities to their Risk Registers, so carbon, energy and waste opportunities are tracked and reviewed alongside the cost and schedule risk review process.

Table 1 – Carbon and Resource Opportunities tracker

**if available*

Hierarchy	Hierarchy principle	Proposal with brief narrative of benefits	Status	Responsible	Status notes	Projected Cost saving*	Other projected savings*
Carbon / Energy / Waste	Hierarchy principle e.g., Build Nothing, Remove fossil fuels, Reuse	Proposed initiative/intervention with a high-level summary of the expected benefits.	Proposed/ Implemented/ Rejected	Entity/role responsible for opportunity	Notes should be based on status: • Proposed – salient points, action to progress • Implemented – point at which (e.g., Detailed Design Review) proposal was implemented. • Rejected – reason why proposal was not adopted. This is to demonstrate the work the project has undertaken and prevent later stages repeating work (or understanding why proposal was initially discounted if item is being revisited).	Cost saved. Quantitative if information available, if not qualitative.	Carbon/ waste/ energy saved. Quantitative if information available, if not qualitative.
Carbon	Build less	Reuse existing material from site as much as is reasonably practicable, such as kerbs and paving slabs.	Proposed	Contractor			
Carbon	Build less	Utilise existing signposts or lighting columns to mount new EV signs.	Proposed	Designer			
Carbon	Build clever	Use fully recyclable bollards, potentially bio-polymer bollards which have less embodied carbon than steel or concrete bollards	Proposed	Designer			
Carbon	Build clever	Use low carbon concrete where possible	Proposed	Designer			
Waste	Reduce	Carry out all required investigations during design stages to de-risk the construction phase.	Proposed	Designer			
Energy	Remove fossil fuels	Use electrically powered plants for construction	Proposed	Contractor			

TfL RESTRICTED

Carbon	Build efficiently	Plan and coordinate works efficiently before going on site	Proposed	Designer/Contractor			
Carbon	Build clever	Introduce remote monitoring of EV charge points to reduce requirements for on site inspections	Proposed	Designer			
Waste	Reduce	Charger uses modular design so module can be swapped out for replacement to minimise waste.	Proposed	Designer			

TfL RESTRICTED

Step 3: Carbon and Resource Trackers

Summary of Whole Life Carbon Models

- The Pathway Stage at which to begin modelling is defined in the digital Environmental Evaluation according to characterisation:
  - Major/Significant – Option Selection
    - Quantitative modelling at longlist and shortlist
  - Standard – Option Selection
    - Qualitative assessment at longlist
    - Quantitative model at shortlist
  - Simple – Concept Design
- For further guidance for Whole Life Carbon Modelling, please review the Carbon Management Training Suite.

Table 2 – Summary of Whole Life Carbon Models

Model	Date produced	Modeller(s) and organisations	Tool(s) used	Major Boundaries and Assumptions	Document Reference(s)
Baseline	*Insert date*		E.g., IStructE carbon tool, TfL Infrastructure Carbon Model Tool, City Planning Carbon Model Tool (eTool) , RSSB Carbon tool etc.		Document references of the Whole Life Carbon Model and any accompanying carbon reports produced.
Concept Design v1	*Insert date*				
Concept Design v2	*Insert date*				
Detailed Design	*Insert date*				
Delivery	*Insert date*				
Add/remove as required					

TfL RESTRICTED

Table 3 – Summary of Whole Life Carbon Model results (tCO2e)

- For further guidance for Whole Life Carbon Modelling, please review the Carbon Management Training Suite.
- Delete or separate lifecycle module columns dependant on the Scope of the project's Whole Life Carbon Models.

Project stage	A0	A1-3	A4	A5	B1	B2-3, 5	B4	B6	B7	B8	C1-4	D	Total	High level narrative
Baseline														
Concept Design v1														
Concept Design v2														
Detailed Design														
Delivery														
Add/remove as required														

Table 4 – Whole Life Carbon Model Hotspots

This table records the hotspots from the current Whole Life Carbon Model. Note that the hotspots may change through the project lifecycle as opportunities and risks and realised.

Hotspot	Description	Estimated Whole Life Carbon emissions (tCO2e)	% of project Whole life Carbon emissions	Description of Table 1 opportunities being pursued that will reduce the impact of the hotspot
Hotspot 1 name	E.g., energy			
Sub-hotspot 1 name	E.g., lighting			
Sub-hotspot 2 name	E.g., HVAC plant			
Hotspot 2 name	E.g., Superstructure			
Hotspot 3 name	E.g., Concrete			
Hotspot 4 name				
Add/remove as required				

TfL RESTRICTED

Summary of Resource Use

This table records the estimated and measured resource usage of a project in absolute terms to aid understanding of the amount of change in Whole Life Carbon Emissions due to application of Build Nothing and Build Less.

Table 5 – Summary of Resource Use

Please add more columns for significant resources used by a project as required (e.g., asphalt, timber, water etc.).

Pathway Stage	Concrete (m^3)	Steel (t)	Asphalt (m^3)	Aggregates (m^3)	Add other key resources here	Add other key resources here	Add other key resources here	High level narrative
Baseline								E.g., Concrete figure only includes superstructure.
Concept Design no. 1 (2021)								
Concept Design no. 2 (2022)								
Detailed Design (2023)								
Delivery (2025)								
Add/remove as required								

TfL RESTRICTED

Summary of Energy Use

This table records the estimated and measured energy consumption and generation of a project in absolute terms.

Table 6 – Summary of Energy Use

Please add more columns for significant energy sources used by a project as required.

Project stage	Construction Electricity Consumption (kWh)	Construction Diesel (litres)	Operational Electricity Consumption (kWh/annum)	Operational Electricity Generation (kWh/annum)[2]	Operational Natural Gas (m^3/annum)	Add other key energy source here	High level narrative
Baseline							
Concept Design no. 1 (2021)							
Concept Design no. 2 (2022)							
Detailed Design (2023)							
Delivery (2025)							
Add/remove as required							

[2] It is TfL strategic policy for all new build structures to install solar photovoltaic panels for electricity generation.

TfL RESTRICTED

Summary of Waste Streams

This table records the estimated and measured waste streams in absolute terms. (The Site Waste Management Plan should be used to track actual waste performance against estimated.)

Table 7a – Summary of Non-Hazardous Waste Streams

Project stage	Quantity (tonnes)	% Reused	% Recycled	% Recovered	% Landfilled	High level narrative
Baseline						*Include brief details of significant sources of waste*
Concept Design no. 1 (2021)						
Concept Design no. 2 (2022)						
Detailed Design (2023)						
Delivery (2025)						
Add/remove as required						

Table 7b – Summary of Hazardous Waste Streams

Project stage	Quantity (tonnes)	% Reused	% Recycled	% Recovered	% Landfilled	High level narrative
Baseline						
Concept Design no. 1 (2021)						
Concept Design no. 2 (2022)						
Detailed Design (2023)						
Delivery (2025)						
Add/remove as required						

TfL RESTRICTED

Table 7c – Summary of Excavated Material

Project stage	Quantity (tonnes)	% Reused	% Recycled	% Recovered	% Landfilled	High level narrative
Baseline						
Concept Design no. 1 (2021)						
Concept Design no. 2 (2022)						
Detailed Design (2023)						
Delivery (2025)						
Add/remove as required						

TfL RESTRICTED

This section is for the use of the TfL PMO Process & Guidance Team only

Product Details

Name:	Carbon and Resource Plan
Document No:	PD0232
SME:	Senior SHE Environment Manager – Corporate Environment
Accountable:	Senior SHE Environment Manager – Corporate Environment
Review Date:	March 2026

Product Version History

Revision	Date	Reason for Change
A1	14/07/2017	Addition of Front Sheet and Pathway Info Sheet.
A2	09/11/2018	TfL Pathway Refresh - Product updated to align with PD0245 (Environmental Evaluation).
A3	04/04/2019	Improved guidance made minor quality of life improvements. Created and signposted SharePoint site.
A4	17/02/2020	Amended ECA and added ability to add tabs.
A5	20/05/2022	Changed to MS Word format (from macro enabled Excel) and other minor changes including general simplification.
A6	13/03/2023	Improved link to Energy, Resource and Waste reduction and simplified tables. Name changed to Carbon and Resource Plan.

Transport for London

Invitation to Quote

Electric Vehicle Infrastructure Delivery (EVID)
Tranche 2, Batch 1

Volume 2

Appendix T

Site Commissioning Checklist

COMMERCIAL IN CONFIDENCE

TfL Restricted

Site Commissioning Checklist

Contract Ref:

Site Name:

Site Address:

Number of chargers installed at site location:

Number of EV bays:

Unique charge asset identifier ID No.:

1. Has the Supplier notified the Buyer 10 working days prior to the date of the Supplier intends site commissioning.

   Yes/No

   Comments:

2. The Supplier shall have completed the electrical testing in accordance with BS 7671, and an Electrical Installation Certification shall be provided for each Charge Point installation, please answer and provide certificate(s) with this form.

   Yes provided/ not provided.

   Comments:

3. The Supplier complete the EV charger manufacture commissioning procedures. Provided record with this form (inclusive of communications links, payment, current charger check/profile).

   Yes provided/not provided.

4. Has the charge point been delivered on site in accordance with the approved detailed designs from the TAA review assurance (Appendix G TfL PR1504 Highways Technical Assurance Process)?

   Yes/No

   Comments:

5. Provide the details of the drawings the Charge point Site was built to in the table below. Include reference to redline drawing and/or as-builts.

Drawing Tile	Drawing Number/Ref	Revision	Redline drawing /as-builts

6. Has the charge point, and associated works been delivered on site in accordance with the planning decision notice and associated drawings?

   Yes/No:

   Comments:

7. Is the charge point operational, clean, safe, and tidy condition?

   Yes/No:

   Comments:

8. Does the charger point display the Supplier customer helpline telephone number and email?

   Yes/No:

   Comments:

<u>Supplier</u>

Name:

Supplier Representative Role:

Signature:

Date:

Transport for London

Invitation to Quote

Electric Vehicle Infrastructure Delivery (EVID)
Tranche 2, Batch 1

Volume 2

Appendix U

Whole Life Carbon Assessment

COMMERCIAL IN CONFIDENCE

TfL Restricted

Whole Life Carbon Assessment Requirements

Quantification Methodology Standard
The Supplier shall use BS EN 15978 (Buildings) or BS EN 17472 (Infrastructure - Environment GWP Performance Only).

Scope
The Supplier shall endeavour to conduct a Whole Life Assessment. The Supplier shall seek approval from the Client to omit lifecycle modules from the Whole life Carbon Assessment.

Boundaries
The Supplier shall seek approval from the Client for their proposed System Boundary of the Whole Life Carbon Assessment, works scope that will be omitted, and treatment of Carbon Risk where design information for bottom-up whole life carb

Assumptions
The Supplier shall seek approval from the Cleint for the assumptions and scenarios used in the Whole Life Carbon Assessment.

The Supplier shall detail how each lifecycle module calculation is conducted.

The Reference Study Period shall be 120 years.

Operational Energy Use calculations shall assume grid decarbonisation. The Supplier shall use Green Book Supplementary Guidance: Valuation of Energy Use and Greenhouse Gas Emissions for Appraisal Table 1. Electricity generation after the year 2100 shall be assumed to be zero carbon. Note: the Green Book does not provide forecasts beyond 2100.

No Product embodied carbon decarbonisation shall be assumed.

Tools
The Supplier shall declare the Whole Life Carbon Assessment tool(s) used.

Data Sources
The Supplier shall detail the data sources used in the Assessment

Categorisation Methods
All elements should be categorised by Uniclass 2015 and a relevant commercial estimating taxonomy, or a combination of taxonomies (single taxonomy preferred):
- Rail Assets: Rail Method of Measurement (RMM) (RMM provided within this Appendix)
- Highways Assets: Method of Measurement for Highways Works (MMHW)
- Buildings Assets: New Rules of Measurement (NRM)
- Other: specify within project assumptions

Uncertainties
The Supplier shall provide commentary about the uncertainties in the Assessment.

Document Management
Whole Life Carbon Assessments shall be owned by the Client for use in future project stages and Corporate reporting. Assessments shall be submitted to the client in a transparent, accessible and editable format.

Reporting

| Categorisation | | | | | B Il-of Quantities | | | | Material and Asset Information | | | | | | A0 Pre-Construction | A1-3 Product | A4 Transport | | | | | |

C2 Waste Transport									C3-4 Waste Processing and Disposal								C5 Effects beyond the System Boundary				Whole Life Carbon	Comment
	Module A	Module A																				
Product - plant and machinery	Module A - weight x distance	Module A - weight x distance (e.g. cement mixer truck)	Module A - weight x distance (e.g. tipper lorry)	Module A - weight x distance (e.g. van)	Module A - weight x distance (e.g. flatbed lorry)	Module A - weight x distance (e.g. pickup truck)	Module A - weight x distance (e.g. low loader)	Module A - weight x distance (e.g. HGV)	Module A - weight x distance (e.g. excavator)	Other - tbc	Module C3 - Waste processing for re-use or recovery	Module C3 - Incineration	Module C3 - Landfill	Module C3 - Waste processing for re-use or recovery	Module C4 - Incineration	Module C4 - Landfill	Module C4 - Other	Module C4 - Other	C3-4 tbc	Module D - Net benefits or loads beyond the system boundary	Module D - Net benefits or loads beyond the system boundary	Module D - Net benefits or loads beyond the system boundary	Module D - Net benefits or loads beyond the system boundary	Whole - Lcycle - tbc	Comment

Ref	Name in Bentley MicroStation
1	Element_Location and_Short_Description
2	Level_4_Rail_Method_of_Measurement_Element
3	B6_Appliance_Wattage
4	B6_Appliance_Power_Factor
5	B6_Annualised_Appliance_Utilisation
6	FORMULA | B6_Carbon_Emissions
7	A1-3_Material_Description
8	A1-3_Carbon_Factor
9	A1-3_Carbon_Factor_Unit
10	A1-3_Carbon_Factor_Source
11	FORMULA | A1-3_Quantity
12	FORMULA | A1-3_Carbon_Emissions
13	A4_Carbon_Factor
14	A4_Carbon_Factor_Unit
15	A4_Carbon_Factor_Source
16	A4_Quantity
17	FORMULA | A4_Carbon_Emissions
18	A5_Carbon_Factor
19	A5_Carbon_Factor_Unit
20	A5_Carbon_Factor_Source
21	A5_Quantity
22	FORMULA | A5_Carbon_Emissions
23	B4_Factored_Service_Life
24	FORMULA | B4_Carbon_Emissions
25	Optional_Carbon_Commentary
26	FORMULA | Sum_of_Carbon_Emissions

Level 4	Level 4 Name
1.01.01.01.01	Consoles and Panels
1.01.01.01.02	Lever Frames
1.01.01.01.03	Ground Frames
1.01.01.01.04	Train Describers
1.01.01.01.05	Supervisory Systems
1.01.01.01.06	Signalling Simulator
1.01.01.02.01	Micro-processor Based Systems
1.01.01.02.02	Electro-mechanical Interlocking
1.01.01.02.03	Mechanical
1.01.01.02.04	Trackside Interlocking Interface Unit
1.01.01.02.05	Tokenless Block
1.01.01.03.01	Electrical
1.01.01.03.02	Hydraulic
1.01.01.03.03	Electro-pneumatic
1.01.01.03.04	Air
1.01.01.03.05	Mechanical
1.01.01.04.01	Colour light signal
1.01.01.04.02	Banner Repeaters
1.01.01.04.03	Position Light Signal
1.01.01.04.04	Route Indicators
1.01.01.04.05	Signal Functions
1.01.01.04.06	Mechanical Signal
1.01.01.04.07	Operational Signs and Noticeboards
1.01.01.04.08	Other
1.01.01.05.01	Track Circuits
1.01.01.05.02	Axle Counters
1.01.01.05.03	Treadles
1.01.01.05.04	Balise
1.01.01.05.05	Insulated Block Joints (IBJs)
1.01.01.05.06	Impedance Bonds
1.01.01.05.07	Hot Axle Box Detectors
1.01.01.06.01	Automatic Warning System (AWS)
1.01.01.06.02	Train Protection Warning System (TPWS)
1.01.01.06.03	Automatic Train Control (ATC)
1.01.01.06.04	Automatic Train Protection (ATP)
1.01.01.07.01	Time Division Data Transmission Systems (TDM)
1.01.01.07.02	Frequency Division Data Transmission Systems (FDM)
1.01.01.07.03	Radio Electronic Tokenless Block (RETB)
1.01.01.07.04	Lockout Device (PLOD)
1.01.01.07.05	Alarms, Warnings and Controls
1.01.01.07.06	Other; state type
1.01.01.08.01	Cables
1.01.01.08.02	Containment in Buildings or Structures
1.01.01.08.03	Tremble Devices / Theft Protection
1.01.01.09.01	Freestanding Single Post: Straight
1.01.01.09.02	Freestanding Single Post: Cranked
1.01.01.09.03	Freestanding Single Post: Lightweight
1.01.01.09.04	Freestanding Single Post: Collapsible
1.01.01.09.05	Fitting; Wall or Roof: state type
1.01.01.09.06	Structural Ancillaries, Fitting to Existing Structures
1.01.01.09.07	Signal Support Structure: Cantilever Single Track
1.01.01.09.08	Signal Support Structure: Cantilever Over 2 Tracks
1.01.01.09.09	Signal Support Structure: Cantilever Over 3 Tracks
1.01.01.09.10	Signal Support Structure: Cantilever Over 4 Tracks
1.01.01.09.11	Signal Support Structure: Gantry / Portal 2 Tracks
1.01.01.09.12	Signal Support Structure: Gantry / Portal 3 Tracks
1.01.01.09.13	Signal Support Structure: Gantry / Portal 4 Tracks
1.01.01.09.14	Signal Support Structure: Gantry / Portal 5 Tracks

1.01.01.09.15	Signal Support Structure: Gantry / Portal 6 Tracks
1.01.01.09.16	Signal Support Structure: Gantry / Portal 7 Tracks
1.01.01.09.17	Signal Support Structure: Gantry / Portal 8 Tracks
1.01.01.09.18	Signal Support Structure: Gantry / Portal 9 Tracks
1.01.01.09.19	Signal Support Structure: Gantry / Portal 10 Tracks
1.01.01.09.20	Immunisation
1.01.01.10.01	Location Case complete with Racking and Equipment: state type
1.01.01.10.02	Portable Building complete with Services
1.01.01.10.03	Trackside Equipment: Level Ground: state type foundation
1.01.01.10.04	Trackside Equipment: Staging: 'Up Bank' for Cut and 'Down Bank' for Embankments: state type, location and foundation
1.01.01.11.01	Stage : state reference
1.01.01.12.01	Fringe : state reference
1.01.01.13.01	Highway Works
1.01.01.13.02	Barriers
1.01.01.13.03	Signal and Traffic Protection
1.01.01.13.04	Controls and Operating Systems: state type
1.01.01.14.01	Testing
1.01.01.14.02	Commissioning and Handover
1.01.01.15.01	Spares: state type
1.01.01.16.01	Materials and Equipment
1.01.02.01.01	Supervisory Control
1.01.02.01.02	Incident Management Systems (IMS)
1.01.02.01.03	Stock and Crew Systems
1.01.02.01.04	Safe Track Worker Access
1.01.02.01.05	Other
1.01.03.01.01	Hardware
1.01.03.01.02	Installation
1.01.03.01.03	Computer Software and System Development
1.01.03.02.01	Testing
1.01.03.02.02	Commissioning and Handover
1.01.04.01.01	Hardware
1.01.04.01.02	Installation
1.01.04.01.03	Computer Software and System Development
1.01.04.02.01	Radio Block Control (RBC)
1.01.04.03.01	Testing
1.01.04.03.02	Commissioning and Handover
1.01.05.01.01	Hardware
1.01.05.01.02	Installation
1.01.05.01.03	Computer Software and System Development
1.01.05.02.01	Hardware
1.01.05.02.02	Installation
1.01.05.02.03	Computer Software and System Development
1.01.05.03.01	Hardware
1.01.05.03.02	Installation
1.01.05.03.03	Computer Software and System Development
1.01.05.04.01	Hardware
1.01.05.04.02	Installation
1.01.05.04.03	Computer Software and System Development
1.01.05.05.01	Hardware
1.01.05.05.02	Installation
1.01.05.05.03	Computer Software and System Development
1.01.05.06.01	Hardware
1.01.05.06.02	Installation
1.01.05.06.03	Computer Software and System Development
1.01.05.07.01	Hardware
1.01.05.07.02	Installation
1.01.05.07.03	Computer Software & System Development
1.01.05.08.01	Hardware
1.01.05.08.02	Installation

1.01.05.08.03	Computer Software and System Development
1.02.01.01.01	Base
1.02.01.01.02	Enclosure
1.02.01.01.03	Compound
1.02.01.01.04	Site Access
1.02.01.01.05	Switchgear Equipment
1.02.01.01.06	Transformers
1.02.01.01.07	Rectifiers
1.02.01.01.08	Protection and Control Equipment
1.02.01.01.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.02.01.01.10	Data Connection to Control Centre
1.02.01.02.01	Base
1.02.01.02.02	Enclosure
1.02.01.02.03	Compound
1.02.01.02.04	Site Access
1.02.01.02.05	Switchgear Equipment
1.02.01.02.06	Transformers
1.02.01.02.07	Rectifiers
1.02.01.02.08	Protection and Control Equipment
1.02.01.02.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.02.01.02.10	Data Connection to Control Centre
1.02.01.03.01	Base
1.02.01.03.02	Enclosure
1.02.01.03.03	Compound
1.02.01.03.04	Site Access
1.02.01.03.05	Switchgear Equipment
1.02.01.03.06	Transformers
1.02.01.03.07	Rectifiers
1.02.01.03.08	Protection and Control Equipment
1.02.01.03.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.02.01.03.10	Data Connection to Control Centre
1.02.01.04.01	Base
1.02.01.04.02	Enclosure
1.02.01.04.03	Compound
1.02.01.04.04	Site Access
1.02.01.04.05	Switchgear Equipment
1.02.01.04.06	Transformers
1.02.01.04.07	Rectifiers
1.02.01.04.08	Protection and Control Equipment
1.02.01.04.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.02.01.04.10	Data Connection to Control Centre
1.02.01.05.01	Base
1.02.01.05.02	Enclosure
1.02.01.05.03	Compound
1.02.01.05.04	Site Access
1.02.01.05.05	Switchgear Equipment
1.02.01.05.06	Transformers
1.02.01.05.07	Rectifiers
1.02.01.05.08	Protection and Control Equipment
1.02.01.05.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.02.01.05.10	Data Connection to Control Centre
1.02.01.06.01	Base
1.02.01.06.02	Enclosure
1.02.01.06.03	Compound
1.02.01.06.04	Site Access
1.02.01.06.05	Switchgear Equipment
1.02.01.06.06	Transformers
1.02.01.06.07	Rectifiers
1.02.01.06.08	Protection and Control Equipment

1.02.01.06.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.02.01.06.10	Data Connection to Control Centre
1.02.01.07.01	Base
1.02.01.07.02	Enclosure
1.02.01.07.03	Compound
1.02.01.07.04	Site Access
1.02.01.07.05	Switchgear Equipment
1.02.01.07.06	Transformers
1.02.01.07.07	Rectifiers
1.02.01.07.08	Protection and Control Equipment
1.02.01.07.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.02.01.07.10	Data Connection to Control Centre
1.02.01.08.01	Base
1.02.01.08.02	Enclosure
1.02.01.08.03	Compound
1.02.01.08.04	Site Access
1.02.01.08.05	Switchgear Equipment
1.02.01.08.06	Transformers
1.02.01.08.07	Rectifiers
1.02.01.08.08	Protection and Control Equipment
1.02.01.08.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.02.01.08.10	Data Connection to Control Centre
1.02.01.09.01	Base
1.02.01.09.02	Enclosure
1.02.01.09.03	Compound
1.02.01.09.04	Site Access
1.02.01.09.05	Switchgear Equipment
1.02.01.09.06	Transformers
1.02.01.09.07	Rectifiers
1.02.01.09.08	Protection and Control Equipment
1.02.01.09.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.02.01.09.10	Data Connection to Control Centre
1.02.01.10.01	Base
1.02.01.10.02	Enclosure
1.02.01.10.03	Compound
1.02.01.10.04	Site Access
1.02.01.10.05	Switchgear Equipment
1.02.01.10.06	Transformers
1.02.01.10.07	Rectifiers
1.02.01.10.08	Protection and Control Equipment
1.02.01.10.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.02.01.10.10	Data Connection to Control Centre
1.02.01.11.01	Base
1.02.01.11.02	Enclosure
1.02.01.11.03	Compound
1.02.01.11.04	Site Access
1.02.01.11.05	Switchgear Equipment
1.02.01.11.06	Transformers
1.02.01.11.07	Rectifiers
1.02.01.11.08	Protection and Control Equipment
1.02.01.11.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.02.01.11.10	Data Connection to Control Centre
1.02.01.12.01	Base
1.02.01.12.02	Enclosure
1.02.01.12.03	Compound
1.02.01.12.04	Site Access
1.02.01.12.05	Switchgear Equipment
1.02.01.12.06	Transformers
1.02.01.12.07	Rectifiers

1.02.01.12.08	Protection and Control Equipment
1.02.01.12.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.02.01.12.10	Data Connection to Control Centre
1.02.01.13.01	Cable
1.02.01.13.02	Containment in Buildings or Structures
1.02.01.13.03	Tremble Devices / Theft Protection
1.02.01.13.04	HV Cable Terminations
1.02.01.14.01	Testing: During the Progress of the Works
1.02.01.14.02	Testing: On Completion of the Works
1.02.01.14.03	Commissioning: Work Completed in Sections
1.02.01.14.04	Commissioning: Co-ordination of Sectional Work
1.02.01.14.05	Commissioning and Handover
1.02.01.15.01	Switchgear Equipment
1.02.01.15.02	Auto Transformers (AT)
1.02.01.15.03	Supervisory Control and Data Acquisition (SCADA) Equipment
1.02.01.15.04	Cables
1.02.02.01.01	Piled Foundation
1.02.02.01.02	Reinforced Concrete Foundation
1.02.02.01.03	Single Track Cantilever
1.02.02.01.04	Twin Track Cantilever
1.02.02.01.05	Twin Cantilever
1.02.02.01.06	Portal
1.02.02.01.07	Anchor Portal
1.02.02.01.08	Mid-point Anchor
1.02.02.01.09	Headspan
1.02.02.01.10	Self-supporting Anchor
1.02.02.01.11	Back-tie
1.02.02.01.12	Structure Number Plate
1.02.02.01.13	Anti-climbing Guard
1.02.02.01.14	Fixings to Bridges and Viaducts
1.02.02.01.15	Fixings to Tunnels
1.02.02.02.01	Support and Registration Assemblies
1.02.02.02.02	Earth Wire Anchor
1.02.02.02.03	Autotransformer 'Gibbet' Steelwork
1.02.02.03.01	Contact Wire
1.02.02.03.02	Catenary Wire
1.02.02.03.03	Contenary Wire
1.02.02.03.04	Current Jumper
1.02.02.03.05	Tensioning Device
1.02.02.04.01	Isolation Devices
1.02.02.04.02	Insulators
1.02.02.04.03	Neutral Sections
1.02.02.05.01	Overhead Tramlines
1.02.02.05.02	Circuit Breaker
1.02.02.05.03	Low Neg Shoe Detector Traction
1.02.02.05.04	Switches
1.02.02.06.01	Return Conductor
1.02.02.06.02	Earthing Conductor
1.02.02.06.03	Support Structure Bonds Ancillary
1.02.02.06.04	Structure Bonds
1.02.02.06.05	Return Screening Conductor
1.02.02.07.01	Return Conductor
1.02.02.07.02	Station Canopies
1.02.02.07.03	Parapets
1.02.02.08.01	Testing: During the Progress of the Works
1.02.02.08.02	Testing: On Completion of the Works
1.02.02.08.03	Commissioning: Work Completed in Sections
1.02.02.08.04	Commissioning: Co-ordination of Sectional Work
1.02.02.08.04	Commissioning and Handover

1.02.02.09.01	Support Structures
1.02.02.09.02	Small Part Steelwork (SPS)
1.02.02.09.03	Wiring
1.02.03.01.01	Conductor Rail
1.02.03.01.02	Return Conductor Rail
1.02.03.01.03	Ramps
1.02.03.01.04	Track Isolating Switch: state type
1.02.03.01.05	Guard Boards
1.02.03.02.01	Flashover Strips
1.02.03.02.02	Rail to Rail Bonds
1.02.03.02.03	Electric Traction Equipment (ETE)
1.02.03.02.04	Structure to Rail Bonds
1.02.03.02.05	Spider Plate Bonds
1.02.03.03.01	Testing: During the Progress of the Works
1.02.03.03.02	Testing: On Completion of the Works
1.02.03.03.03	Commissioning: Work Completed in Sections
1.02.03.03.04	Commissioning: Co-ordination of Sectional Work
1.02.03.03.05	Commissioning and Handover
1.02.03.04.01	Contact Rail System: state details
1.02.03.04.02	Earthing and Bonding : state details
1.03.01.01.01	Base
1.03.01.01.02	Enclosure
1.03.01.01.03	Compound
1.03.01.01.04	Site Access
1.03.01.01.05	Substation Equipment
1.03.01.01.06	Transformers
1.03.01.01.07	Rectifiers
1.03.01.01.08	Protection and Control Equipment
1.03.01.01.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.03.01.01.10	Data Connection to Control Centre
1.03.01.02.01	Base
1.03.01.02.02	Enclosure
1.03.01.02.03	Compound
1.03.01.02.04	Site Access
1.03.01.02.05	Substation Equipment
1.03.01.02.06	Transformers
1.03.01.02.07	Rectifiers
1.03.01.02.08	Protection and Control Equipment
1.03.01.02.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.03.01.02.10	Data Connection to Control Centre
1.03.01.03.01	Base
1.03.01.03.02	Enclosure
1.03.01.03.03	Compound
1.03.01.03.04	Site Access
1.03.01.03.05	Substation Equipment
1.03.01.03.06	Transformers
1.03.01.03.07	Rectifiers
1.03.01.03.08	Protection and Control Equipment
1.03.01.03.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.03.01.03.10	Data Connection to Control Centre
1.03.01.04.01	Base
1.03.01.04.02	Enclosure
1.03.01.04.03	Compound
1.03.01.04.04	Site Access
1.03.01.04.05	Substation Equipment
1.03.01.04.06	Transformers
1.03.01.04.07	Rectifiers
1.03.01.04.08	Protection and Control Equipment
1.03.01.04.09	Supervisory Control and Data Acquisition (SCADA) Equipment

1.03.01.04.10	Data Connection to Control Centre
1.03.01.05.01	DNO Power Cubicle
1.03.01.05.02	Principal Supply Point (PSP)
1.03.01.05.03	Auxiliary Supply Points (ASP)
1.03.01.05.04	Functional Supply Points (FSP)
1.03.01.05.05	Feeder Protection Panel
1.03.01.06.01	Isolation Devices
1.03.01.06.02	Insulators
1.03.01.06.03	Earthing
1.03.01.06.04	Lightning Protection
1.03.01.06.05	Main Protective Bonding Conductor
1.03.01.06.06	Supplementary Bonding Conductors
1.03.01.07.01	Cable
1.03.01.07.02	Containment in Buildings or Structures
1.03.01.08.01	Testing: During the Progress of the works
1.03.01.08.02	Testing: On completion of the works
1.03.01.08.03	Commissioning: Work completed in sections
1.03.01.08.04	Commissioning: Co-ordination of Sectional Work
1.03.01.08.05	Commissioning and Handover
1.03.01.09.01	Sub-station Equipment
1.03.01.09.02	Transformer
1.03.01.09.03	Rectifier
1.03.01.09.04	Protection and Control Equipment
1.03.01.09.05	Supervisory Control and Data Acquisition (SCADA) Equipment
1.03.01.09.06	Cables
1.03.02.01.01	Rail Heaters
1.03.02.01.02	Points Heaters
1.03.02.01.03	Junction Lighting
1.03.02.02.01	General Equipment
1.03.02.02.02	Workshop Equipment
1.03.02.02.03	Cleaning Equipment
1.03.02.02.04	Lifting Equipment
1.03.02.02.05	De-icing Equipment
1.03.02.02.06	Overhead Trolley
1.03.02.02.07	Access Equipment
1.03.02.02.08	Battery Equipment
1.03.02.02.09	Compressed Air Equipment
1.03.02.02.10	Calibration
1.03.02.02.11	Gauge Equipment
1.03.02.02.12	Train Test Equipment
1.03.02.02.13	Train Monitoring Equipment
1.03.02.02.14	Welding Equipment
1.03.02.02.15	Safety Equipment
1.03.02.02.16	Wheel Lathe
1.03.02.02.17	Electrical Portable Appliances
1.03.02.03.01	Chemical Effluent Toilet (CET) Point
1.03.02.03.02	Carriage Washing Plant
1.03.02.03.03	Carriage Watering System
1.03.02.03.04	Sanding System Point
1.03.02.03.05	Diesel Fuelling Point
1.03.02.04.01	Testing: During the Progress of the Works
1.03.02.04.02	Testing: On Completion of the Works
1.03.02.04.03	Commissioning: Work Completed in Sections
1.03.02.04.04	Commissioning: Co-ordination of Sectional Work
1.03.02.04.05	Commissioning and Handover
1.03.02.05.01	Lineside Equipment
1.03.02.05.02	Maintenance Equipment
1.03.02.05.03	Operational Equipment
1.03.02.05.04	Depot Traction

1.04.01.01.01	Track Ballast: state width and depth
1.04.01.01.02	Sleepers: state type, fixings and spacing
1.04.01.01.03	Running Rails: state profile, jointing type and curvature
1.04.01.02.01	Track Slab: state section and reinforcement details
1.04.01.02.02	Sleepers: state type, fixings and spacing
1.04.01.02.03	Running Rails: state profile, jointing type and curvature
1.04.01.03.01	Longitudinal Bearers: state type, fixings and section
1.04.01.03.02	Sleepers: state type, fixings and spacing
1.04.01.03.03	Running Rails: state profile, jointing type and curvature
1.04.01.04.01	Check Rails: state type
1.04.01.04.02	Guard Rails: state type
1.04.01.04.03	Rail Lubricators: state type
1.04.01.04.04	Cable Management Sleepers
1.04.01.04.05	Buffer Stops
1.04.01.04.06	Other Ancillaries
1.04.02.01.01	Trap
1.04.02.01.02	Turnout
1.04.02.01.03	Crossover
1.04.02.01.04	Diamond: state type
1.04.02.01.05	Scissor Crossover
1.04.02.01.06	Double Junction: Diamond: state type
1.04.02.01.07	Three Line Crossover: Diamond: state type
1.04.02.01.08	Tandem Turnout
1.04.02.01.09	Other: state type, size and details
1.04.02.02.01	Trap
1.04.02.02.02	Turnout
1.04.02.02.03	Crossover
1.04.02.02.04	Diamond: state type
1.04.02.02.05	Scissor Crossover
1.04.02.02.06	Double Junction: Diamond: state type
1.04.02.02.07	Three Line Crossover: Diamond: state type
1.04.02.02.08	Tandem Turnout
1.04.02.02.09	Other: state type, size and details
1.04.02.03.01	Trap
1.04.02.03.02	Turnout
1.04.02.03.03	Crossover
1.04.02.03.04	Diamond: state type
1.04.02.03.05	Scissor Crossover
1.04.02.03.06	Double Junction: Diamond: state type
1.04.02.03.07	Three Line Crossover: Diamond: state type
1.04.02.03.08	Tandem Turnout
1.04.02.03.09	Other: state type, size and details
1.04.02.04.01	Cable Management Sleepers
1.04.02.04.02	Lateral Resistance Plates
1.04.02.04.03	Sand Drag: state dimensions
1.04.02.04.04	Other Ancillaries: state type
1.04.03.01.01	Ballast Track
1.04.03.01.02	Longitudinal Bearer Track
1.04.03.01.03	Ancillaries: state type
1.04.03.02.01	Switches and Crossing: state layout
1.04.03.02.02	Ancillaries: state type
1.04.04.01.01	Ballast Track
1.04.04.01.02	Slab Track
1.04.04.01.03	Longitudinal Bearer Track
1.04.04.01.04	Ancillaries
1.04.04.02.01	Switches and Crossing: state size and layout
1.04.04.02.02	Ancillaries
1.05.01.01.01	State type and model reference
1.05.01.02.01	State type and model reference

1.05.02.01.01	Masts
1.05.02.01.02	Aerials
1.05.02.01.03	Base Stations
1.05.03.01.01	State type
1.05.03.02.01	PCM: Digital
1.05.03.02.02	Drop and Insert: Digital Circuit
1.05.03.02.03	Carrier: Analogue
1.05.04.01.01	Conductor
1.05.04.02.01	Conductor
1.05.04.03.01	Conductor
1.05.04.04.01	Conductor
1.05.05.01.01	Large > 64 Lines
1.05.05.01.02	Medium 32 to 64 Lines
1.05.05.01.03	Small < 32 Lines
1.05.05.02.01	Large > 64 Lines
1.05.05.02.02	Medium 32 to 64 Lines
1.05.05.02.03	Small < 32 Lines
1.05.05.03.01	Large > 64 Lines
1.05.05.03.02	Medium 32 to 64 Lines
1.05.05.03.03	Small < 32 Lines
1.05.05.04.01	Large > 64 Lines
1.05.05.04.02	Medium 32 to 64 Lines
1.05.05.04.03	Small < 32 Lines
1.05.06.01.01	State type and model reference
1.05.06.02.01	State type and model reference
1.05.06.03.01	State type and model reference
1.05.06.04.01	State type and model reference
1.05.06.05.01	State type and model reference
1.05.06.06.01	State type and model reference
1.05.06.07.01	State type and model reference
1.05.06.08.01	State type and model reference
1.05.06.09.01	State type and model reference
1.05.06.10.01	State type and model reference
1.05.07.01.01	CCTV Cameras
1.05.07.01.02	Monitors
1.05.07.01.03	Mirrors
1.05.07.01.04	Control Panels
1.05.07.01.05	Microphones and Speaking Points
1.05.07.01.06	Recorders
1.05.07.01.07	Amplifiers
1.05.07.01.08	Primary Object Detectors (POD)
1.05.07.01.09	Complementary Object Detectors (COD)
1.05.07.02.01	CCTV Cameras
1.05.07.02.02	Monitors
1.05.07.02.03	Mirrors
1.05.07.02.04	Control Panels
1.05.07.02.05	Microphones and Speaking Points
1.05.07.02.06	Recorders
1.05.07.02.07	Amplifiers
1.05.07.02.08	Primary Object Detectors (POD)
1.05.07.02.09	Complementary Object Detectors (COD)
1.05.07.03.01	CCTV Cameras
1.05.07.03.02	Monitors
1.05.07.03.03	Mirrors
1.05.07.03.04	Control Panels
1.05.07.03.05	Microphones and Speaking Points
1.05.07.03.06	Recorders
1.05.07.03.07	Amplifiers
1.05.07.03.08	Primary Object Detectors (POD)

1.05.07.03.09	Complementary Object Detectors (COD)
1.05.07.04.01	CCTV Cameras
1.05.07.04.02	Monitors
1.05.07.04.03	Mirrors
1.05.07.04.04	Control Panels
1.05.07.04.05	Microphones and Speaking Points
1.05.07.04.06	Recorders
1.05.07.04.07	Amplifiers
1.05.07.04.08	Primary Object Detectors (POD)
1.05.07.04.09	Complementary Object Detectors (COD)
1.05.08.01.01	Automatic Train Reporting (ATR)
1.05.08.01.02	Station Information VDU Stepping (SIVS)
1.05.08.01.03	Train Running Under System TOPS (TRUST)
1.05.09.01.01	Point Heaters
1.05.09.01.02	Standby Generators
1.05.09.01.03	Pumps
1.05.09.01.04	SCADA Installation
1.05.09.01.05	Relocatable Equipment Buildings (REB)
1.05.09.02.01	Point Heaters
1.05.09.02.02	Standby Generators
1.05.09.02.03	Pumps
1.05.09.02.04	SCADA Installation
1.05.09.02.05	Relocatable Equipment Buildings (REB)
1.05.10.01.01	Speakers
1.05.10.01.02	Microphones and Speaking Points
1.05.10.01.03	Amplifier
1.05.10.01.04	Ambient Noise Sensor
1.05.10.01.05	Control Panels
1.05.10.02.01	Video Display Units
1.05.10.02.02	Recorders
1.05.10.02.03	Control Panels
1.05.10.03.01	Analogue
1.05.10.03.02	Digital
1.05.11.01.01	Housing
1.05.11.01.02	Racking
1.05.11.01.03	Services
1.05.11.01.04	Foundation
1.05.11.02.01	Housing
1.05.11.02.02	Racking
1.05.11.02.03	Services
1.05.11.02.04	Foundation
1.05.11.03.01	Housing
1.05.11.03.02	Racking
1.05.11.03.03	Services
1.05.11.03.04	Foundation
1.05.11.04.01	Housing
1.05.11.04.02	Racking
1.05.11.04.03	Services
1.05.11.04.04	Foundation
1.05.12.01.01	Phased: state timing
1.05.12.01.02	On Completion
1.05.12.02.01	Phased: state timing
1.05.12.02.02	On Completion
1.05.12.03.01	Phased: state timing
1.05.12.03.02	On Completion
1.05.12.04.01	Phased: state timing
1.05.12.04.02	On Completion
1.05.12.05.01	Phased: state timing
1.05.12.05.02	On Completion

1.05.13.01.01	State system spares required
1.05.14.01.01	Abandonment
1.05.14.01.02	Recovery
1.05.14.01.03	Disposal of Redundant Equipment
1.05.14.02.01	Abandonment
1.05.14.02.02	Recovery
1.05.14.02.03	Disposal of Redundant Equipment
1.05.14.03.01	Abandonment
1.05.14.03.02	Recovery
1.05.14.03.03	Disposal of Redundant Equipment
1.05.14.04.01	Abandonment
1.05.14.04.02	Recovery
1.05.14.04.03	Disposal of Redundant Equipment
1.05.14.05.01	Abandonment
1.05.14.05.02	Recovery
1.05.14.05.03	Disposal of Redundant Equipment
1.05.14.06.01	Abandonment
1.05.14.06.02	Recovery
1.05.14.06.03	Disposal of Redundant Equipment
1.05.14.07.01	Abandonment
1.05.14.07.02	Recovery
1.05.14.07.03	Disposal of Redundant Equipment
1.05.14.08.01	Abandonment
1.05.14.08.02	Recovery
1.05.14.08.03	Disposal of Redundant Equipment
1.05.14.09.01	Abandonment
1.05.14.09.02	Recovery
1.05.14.09.03	Disposal of Redundant Equipment
1.05.14.10.01	Abandonment
1.05.14.10.02	Recovery
1.05.14.10.03	Disposal of Redundant Equipment
1.05.14.11.01	Abandonment
1.05.14.11.02	Recovery
1.05.14.11.03	Disposal of Redundant Equipment
1.06.01.01.01	Standard Foundations
1.06.01.01.02	Specialist Foundations
1.06.01.01.03	Lowest Floor Construction
1.06.01.01.04	Basement Excavation
1.06.01.01.05	Basement Retaining Walls
1.06.02.01.01	Steel Frames
1.06.02.01.02	Space Frames / Decks
1.06.02.01.03	Concrete Casings to Steel Frames
1.06.02.01.04	Concrete Frames
1.06.02.01.05	Timber Frames
1.06.02.01.06	Specialist Frames
1.06.02.02.01	Floors
1.06.02.02.02	Balconies
1.06.02.02.03	Drainage to Balconies
1.06.02.03.01	Roof Structure
1.06.02.03.02	Roof Coverings
1.06.02.03.03	Specialist Roof Systems
1.06.02.03.04	Roof Drainage
1.06.02.03.05	Roof Lights, Skylights and Openings
1.06.02.03.06	Roof Features
1.06.02.04.01	Stair / Ramp Structures
1.06.02.04.02	Stair / Ramp Finishes
1.06.02.04.03	Stair / Ramp Balustrades and Handrails
1.06.02.04.04	Ladders / Chutes / Slides
1.06.02.05.01	External Enclosing Walls above Ground Level

1.06.02.05.02	External Enclosing Walls below Ground Level
1.06.02.05.03	Solar / Rain Screening
1.06.02.05.04	External Soffits
1.06.02.05.05	Subsidiary Walls, Balustrades and Proprietary Balconies
1.06.02.05.06	Façade Access / Cleaning Systems
1.06.02.06.01	External Windows
1.06.02.06.02	External Doors
1.06.02.07.01	Walls and Partitions
1.06.02.07.02	Balustrades and Handrails
1.06.02.07.03	Moveable Room Dividers
1.06.02.07.04	Cubicles
1.06.02.08.01	Internal Doors
1.06.03.01.01	Wall Finishes
1.06.03.02.01	Finishes to Floors
1.06.03.02.02	Raised Access Floors
1.06.03.03.01	Finishes to Ceilings
1.06.03.03.02	False Ceilings
1.06.03.03.03	Demountable Suspended Ceilings
1.06.04.01.01	General Fittings, Furnishings and Equipment
1.06.04.01.02	Domestic Kitchen Fittings and Equipment
1.06.04.01.03	Special Purpose Fittings, Furnishings and Equipment
1.06.04.01.04	Signs / Notices
1.06.04.01.05	Works of Art
1.06.04.01.06	Non-mechanical and Non-electrical Equipment
1.06.04.01.07	Internal Planting
1.06.04.01.08	Bird and Vermin Control
1.06.05.01.01	Sanitary Appliances
1.06.05.01.02	Sanitary Ancillaries
1.06.05.02.01	Services Equipment
1.06.05.03.01	Foul Drainage Above Ground
1.06.05.03.02	Chemical, Toxic and Industrial Waste Drainage
1.06.05.03.03	Refuse Disposal
1.06.05.04.01	Mains Water Supply
1.06.05.04.02	Cold Water Distribution
1.06.05.04.03	Hot Water Distribution
1.06.05.04.04	Local Hot Water Distribution
1.06.05.04.05	Steam and Condensate Distribution
1.06.05.05.01	Heat Source
1.06.05.06.01	Central Heating
1.06.05.06.02	Local Heating
1.06.05.06.03	Central Cooling
1.06.05.06.04	Local Cooling
1.06.05.06.05	Central Heating and Cooling
1.06.05.06.06	Local Heating and Cooling
1.06.05.06.07	Central Air Conditioning
1.06.05.06.08	Local Air Conditioning
1.06.05.07.01	Central Ventilation
1.06.05.07.02	Local and Special Ventilation
1.06.05.07.03	Smoke Extract / Control
1.06.05.08.01	Electrical Mains and Sub-mains Distribution
1.06.05.08.02	Power Installations
1.06.05.08.03	Lighting Installations
1.06.05.08.04	Specialist Lighting Installations
1.06.05.08.05	Local Electricity Generation Systems
1.06.05.08.06	Earthing and Bonding Systems
1.06.05.09.01	Fuel Storage
1.06.05.09.02	Fuel Distribution Systems
1.06.05.10.01	Lifts and Enclosed Hoists
1.06.05.10.02	Escalators

1.06.05.10.03	Moving Pavements
1.06.05.10.04	Powered Stair lifts
1.06.05.10.05	Conveyors
1.06.05.10.06	Dock Levellers and Scissor Lifts
1.06.05.10.08	Car Lifts, Car Stacking Systems, Turntables and the like
1.06.05.10.09	Document Handling Systems
1.06.05.10.10	Other Lift and Conveyor Systems
1.06.05.11.01	Fire Fighting Systems
1.06.05.11.02	Fire Suppression Systems
1.06.05.11.03	Lightning Protection
1.06.05.12.01	Central Control / Building Management Systems
1.06.05.13.01	Specialist Piped Supply Installation
1.06.05.13.02	Specialist Refrigeration Systems
1.06.05.13.03	Specialist Mechanical Installations
1.06.05.13.04	Specialist Electrical / Electronic Installations
1.06.05.13.05	Water Features
1.06.05.13.06	Specialist Station Equipment
1.06.05.14.01	Builder's Work in Connection with Services
1.06.06.01.01	Sanitary Appliances
1.06.06.01.02	Sanitary Ancillaries
1.06.06.02.01	Services Equipment
1.06.06.03.01	Foul Drainage Above Ground
1.06.06.03.02	Chemical, Toxic and Industrial Waste Drainage
1.06.06.03.03	Refuse Disposal
1.06.06.04.01	Mains Water Supply
1.06.06.04.02	Cold Water Distribution
1.06.06.04.03	Hot Water Distribution
1.06.06.04.04	Local Hot Water Distribution
1.06.06.04.05	Steam and Condensate Distribution
1.06.06.05.01	Heat Source
1.06.06.06.01	Central Heating
1.06.06.06.02	Local Heating
1.06.06.06.03	Central Cooling
1.06.06.06.04	Local Cooling
1.06.06.06.05	Central Heating and Cooling
1.06.06.06.06	Local Heating and Cooling
1.06.06.06.07	Central Air Conditioning
1.06.06.06.08	Local Air Conditioning
1.06.06.07.01	Central Ventilation
1.06.06.07.02	Local and Special Ventilation
1.06.06.07.03	Smoke Extract / Control
1.06.06.08.01	Electrical Mains and Sub-mains Distribution
1.06.06.08.02	Power Installations
1.06.06.08.03	Lighting Installations
1.06.06.08.04	Specialist Lighting Installations
1.06.06.08.05	Local Electricity Generation Systems
1.06.06.08.06	Earthing and Bonding Systems
1.06.06.09.01	Fuel Storage
1.06.06.09.02	Fuel Distribution Systems
1.06.06.10.01	Lifts and Enclosed Hoists
1.06.06.10.02	Escalators
1.06.06.10.03	Moving Pavements
1.06.06.10.04	Powered Stair lifts
1.06.06.10.05	Conveyors
1.06.06.10.06	Dock Levellers and Scissor Lifts
1.06.06.10.07	Cranes and Unenclosed Hoists
1.06.06.10.08	Car Lifts, Car Stacking Systems, Turntables and the like
1.06.06.10.09	Document Handling Systems
1.06.06.10.10	Other Lift and Conveyor Systems

1.06.06.11.01	Fire Fighting Systems
1.06.06.11.02	Fire Suppression Systems
1.06.06.11.03	Lightning Protection
1.06.06.12.01	Central Control / Building Management Systems
1.06.06.13.01	Specialist Piped Supply Installation
1.06.06.13.02	Specialist Refrigeration Systems
1.06.06.13.03	Specialist Mechanical Installations
1.06.06.13.04	Specialist Electrical / Electronic Installations
1.06.06.13.05	Water Features
1.06.06.13.06	Specialist Station Equipment
1.06.06.14.01	Builder's Work in Connection with Services
1.06.07.01.01	Sanitary Appliances
1.06.07.01.02	Sanitary Ancillaries
1.06.07.02.01	Services Equipment
1.06.07.03.01	Foul Drainage Above Ground
1.06.07.03.02	Chemical, Toxic and Industrial Waste Drainage
1.06.07.03.03	Refuse Disposal
1.06.07.04.01	Mains Water Supply
1.06.07.04.02	Cold Water Distribution
1.06.07.04.03	Hot Water Distribution
1.06.07.04.04	Local Hot Water Distribution
1.06.07.04.05	Steam and Condensate Distribution
1.06.07.05.01	Heat Source
1.06.07.06.01	Central Heating
1.06.07.06.02	Local Heating
1.06.07.06.03	Central Cooling
1.06.07.06.04	Local Cooling
1.06.07.06.05	Central Heating and Cooling
1.06.07.06.06	Local Heating and Cooling
1.06.07.06.07	Central Air Conditioning
1.06.07.06.08	Local Air Conditioning
1.06.07.07.01	Central Ventilation
1.06.07.07.02	Local and Special Ventilation
1.06.07.07.03	Smoke Extract / Control
1.06.07.08.01	Electrical Mains and Sub-mains Distribution
1.06.07.08.02	Power Installations
1.06.07.08.03	Lighting Installations
1.06.07.08.04	Specialist Lighting Installations
1.06.07.08.05	Local Electricity Generation Systems
1.06.07.08.06	Earthing and Bonding Systems
1.06.07.09.01	Fuel Storage
1.06.07.09.02	Fuel Distribution Systems
1.06.07.10.01	Lifts and Enclosed Hoists
1.06.07.10.02	Escalators
1.06.07.10.03	Moving Pavements
1.06.07.10.04	Powered Stair lifts
1.06.07.10.05	Conveyors
1.06.07.10.06	Dock Levellers and Scissor Lifts
1.06.07.10.07	Cranes and Unenclosed Hoists
1.06.07.10.08	Car Lifts, Car Stacking Systems, Turntables and the like
1.06.07.10.09	Document Handling Systems
1.06.07.10.10	Other Lift and Conveyor Systems
1.06.07.11.01	Fire Fighting Systems
1.06.07.11.02	Fire Suppression Systems
1.06.07.11.03	Lightning Protection
1.06.07.12.01	Central Control / Building Management Systems
1.06.07.13.01	Specialist Piped Supply Installation
1.06.07.13.02	Specialist Refrigeration Systems
1.06.07.13.03	Specialist Mechanical Installations

1.06.07.13.04	Specialist Electrical / Electronic Installations
1.06.07.13.05	Water Features
1.06.07.13.06	Specialist Station Equipment
1.06.07.14.01	Builder's Work in Connection with Services
1.06.08.01.01	Sanitary Appliances
1.06.08.01.02	Sanitary Ancillaries
1.06.08.02.01	Services Equipment
1.06.08.03.01	Foul Drainage Above Ground
1.06.08.03.02	Chemical, Toxic and Industrial Waste Drainage
1.06.08.03.03	Refuse Disposal
1.06.08.04.01	Mains Water Supply
1.06.08.04.02	Cold Water Distribution
1.06.08.04.03	Hot Water Distribution
1.06.08.04.04	Local Hot Water Distribution
1.06.08.04.05	Steam and Condensate Distribution
1.06.08.05.01	Heat Source
1.06.08.06.01	Central Heating
1.06.08.06.02	Local Heating
1.06.08.06.03	Central Cooling
1.06.08.06.04	Local Cooling
1.06.08.06.05	Central Heating and Cooling
1.06.08.06.06	Local Heating and Cooling
1.06.08.06.07	Central Air Conditioning
1.06.08.06.08	Local Air Conditioning
1.06.08.07.01	Central Ventilation
1.06.08.07.02	Local and Special Ventilation
1.06.08.07.03	Smoke Extract / Control
1.06.08.08.01	Electrical Mains and Sub-mains Distribution
1.06.08.08.02	Power Installations
1.06.08.08.03	Lighting Installations
1.06.08.08.04	Specialist Lighting Installations
1.06.08.08.05	Local Electricity Generation Systems
1.06.08.08.06	Earthing and Bonding Systems
1.06.08.09.01	Fuel Storage
1.06.08.09.02	Fuel Distribution Systems
1.06.08.10.01	Lifts and Enclosed Hoists
1.06.08.10.02	Escalators
1.06.08.10.03	Moving Pavements
1.06.08.10.04	Powered Stair lifts
1.06.08.10.05	Conveyors
1.06.08.10.06	Dock Levellers and Scissor Lifts
1.06.08.10.07	Cranes and Unenclosed Hoists
1.06.08.10.08	Car Lifts, Car Stacking Systems, Turntables and the like
1.06.08.10.09	Document Handling Systems
1.06.08.10.10	Other Lift and Conveyor Systems
1.06.08.11.01	Fire Fighting Systems
1.06.08.11.02	Fire Suppression Systems
1.06.08.11.03	Lightning Protection
1.06.08.12.01	Central Control / Building Management Systems
1.06.08.13.01	Specialist Piped Supply Installation
1.06.08.13.02	Specialist Refrigeration Systems
1.06.08.13.03	Specialist Mechanical Installations
1.06.08.13.04	Specialist Electrical / Electronic Installations
1.06.08.13.05	Water Features
1.06.08.13.06	Specialist Station Equipment
1.06.08.14.01	Builder's Work in Connection with Services
1.06.09.01.01	Sanitary Appliances
1.06.09.01.02	Sanitary Ancillaries
1.06.09.02.01	Services Equipment

1.06.09.03.01	Foul Drainage Above Ground
1.06.09.03.02	Chemical, Toxic and Industrial Waste Drainage
1.06.09.03.03	Refuse Disposal
1.06.09.04.01	Mains Water Supply
1.06.09.04.02	Cold Water Distribution
1.06.09.04.03	Hot Water Distribution
1.06.09.04.04	Local Hot Water Distribution
1.06.09.04.05	Steam and Condensate Distribution
1.06.09.05.01	Heat Source
1.06.09.06.01	Central Heating
1.06.09.06.02	Local Heating
1.06.09.06.03	Central Cooling
1.06.09.06.04	Local Cooling
1.06.09.06.05	Central Heating and Cooling
1.06.09.06.06	Local Heating and Cooling
1.06.09.06.07	Central Air Conditioning
1.06.09.06.08	Local Air Conditioning
1.06.09.07.01	Central Ventilation
1.06.09.07.02	Local and Special Ventilation
1.06.09.07.03	Smoke Extract / Control
1.06.09.08.01	Electrical Mains and Sub-mains Distribution
1.06.09.08.02	Power Installations
1.06.09.08.03	Lighting Installations
1.06.09.08.04	Specialist Lighting Installations
1.06.09.08.05	Local Electricity Generation Systems
1.06.09.08.06	Earthing and Bonding Systems
1.06.09.09.01	Fuel Storage
1.06.09.09.02	Fuel Distribution Systems
1.06.09.10.01	Lifts and Enclosed Hoists
1.06.09.10.02	Escalators
1.06.09.10.03	Moving Pavements
1.06.09.10.04	Powered Stair lifts
1.06.09.10.05	Conveyors
1.06.09.10.06	Dock Levellers and Scissor Lifts
1.06.09.10.07	Cranes and Unenclosed Hoists
1.06.09.10.08	Car Lifts, Car Stacking Systems, Turntables and the like
1.06.09.10.09	Document Handling Systems
1.06.09.10.10	Other Lift and Conveyor Systems
1.06.09.11.01	Fire Fighting Systems
1.06.09.11.02	Fire Suppression Systems
1.06.09.11.03	Lightning Protection
1.06.09.12.01	Central Control / Building Management Systems
1.06.09.13.01	Specialist Piped Supply Installation
1.06.09.13.02	Specialist Refrigeration Systems
1.06.09.13.03	Specialist Mechanical Installations
1.06.09.13.04	Specialist Electrical / Electronic Installations
1.06.09.13.05	Water Features
1.06.09.13.06	Specialist Station Equipment
1.06.09.14.01	Builder's Work in Connection with Services
1.06.10.01.01	Sanitary Appliances
1.06.10.01.02	Sanitary Ancillaries
1.06.10.02.01	Services Equipment
1.06.10.03.01	Foul Drainage Above Ground
1.06.10.03.02	Chemical, Toxic and Industrial Waste Drainage
1.06.10.03.03	Refuse Disposal
1.06.10.04.01	Mains Water Supply
1.06.10.04.02	Cold Water Distribution
1.06.10.04.03	Hot Water Distribution
1.06.10.04.04	Local Hot Water Distribution

1.06.10.04.05	Steam and Condensate Distribution
1.06.10.05.01	Heat Source
1.06.10.06.01	Central Heating
1.06.10.06.02	Local Heating
1.06.10.06.03	Central Cooling
1.06.10.06.04	Local Cooling
1.06.10.06.05	Central Heating and Cooling
1.06.10.06.06	Local Heating and Cooling
1.06.10.06.07	Central Air Conditioning
1.06.10.06.08	Local Air Conditioning
1.06.10.07.01	Central Ventilation
1.06.10.07.02	Local and Special Ventilation
1.06.10.07.03	Smoke Extract / Control
1.06.10.08.01	Electrical Mains and Sub-mains Distribution
1.06.10.08.02	Power Installations
1.06.10.08.03	Lighting Installations
1.06.10.08.04	Specialist Lighting Installations
1.06.10.08.05	Local Electricity Generation Systems
1.06.10.08.06	Earthing and Bonding Systems
1.06.10.09.01	Fuel Storage
1.06.10.09.02	Fuel Distribution Systems
1.06.10.10.01	Lifts and Enclosed Hoists
1.06.10.10.02	Escalators
1.06.10.10.03	Moving Pavements
1.06.10.10.04	Powered Stair lifts
1.06.10.10.05	Conveyors
1.06.10.10.06	Dock Levellers and Scissor Lifts
1.06.10.10.07	Cranes and Unenclosed Hoists
1.06.10.10.08	Car Lifts, Car Stacking Systems, Turntables and the like
1.06.10.10.09	Document Handling Systems
1.06.10.10.10	Other Lift and Conveyor Systems
1.06.10.11.01	Fire Fighting Systems
1.06.10.11.02	Fire Suppression Systems
1.06.10.11.03	Lightning Protection
1.06.10.12.01	Central Control / Building Management Systems
1.06.10.13.01	Specialist Piped Supply Installation
1.06.10.13.02	Specialist Refrigeration Systems
1.06.10.13.03	Specialist Mechanical Installations
1.06.10.13.04	Specialist Electrical / Electronic Installations
1.06.10.13.05	Water Features
1.06.10.13.06	Specialist Station Equipment
1.06.10.14.01	Builder's Work in Connection with Services
1.06.11.01.01	Sanitary Appliances
1.06.11.01.02	Sanitary Ancillaries
1.06.11.02.01	Services Equipment
1.06.11.03.01	Foul Drainage Above Ground
1.06.11.03.02	Chemical, Toxic and Industrial Waste Drainage
1.06.11.03.03	Refuse Disposal
1.06.11.04.01	Mains Water Supply
1.06.11.04.02	Cold Water Distribution
1.06.11.04.03	Hot Water Distribution
1.06.11.04.04	Local Hot Water Distribution
1.06.11.04.05	Steam and Condensate Distribution
1.06.11.05.01	Heat Source
1.06.11.06.01	Central Heating
1.06.11.06.02	Local Heating
1.06.11.06.03	Central Cooling
1.06.11.06.04	Local Cooling
1.06.11.06.05	Central Heating and Cooling

1.06.11.06.06	Local Heating and Cooling
1.06.11.06.07	Central Air Conditioning
1.06.11.06.08	Local Air Conditioning
1.06.11.07.01	Central Ventilation
1.06.11.07.02	Local and Special Ventilation
1.06.11.07.03	Smoke Extract / Control
1.06.11.08.01	Electrical Mains and Sub-mains Distribution
1.06.11.08.02	Power Installations
1.06.11.08.03	Lighting Installations
1.06.11.08.04	Specialist Lighting Installations
1.06.11.08.05	Local Electricity Generation Systems
1.06.11.08.06	Earthing and Bonding Systems
1.06.11.09.01	Fuel Storage
1.06.11.09.02	Fuel Distribution Systems
1.06.11.10.01	Lifts and Enclosed Hoists
1.06.11.10.02	Escalators
1.06.11.10.03	Moving Pavements
1.06.11.10.04	Powered Stair lifts
1.06.11.10.05	Conveyors
1.06.11.10.06	Dock Levellers and Scissor Lifts
1.06.11.10.07	Cranes and Unenclosed Hoists
1.06.11.10.08	Car Lifts, Car Stacking Systems, Turntables and the like
1.06.11.10.09	Document Handling Systems
1.06.11.10.10	Other Lift and Conveyor Systems
1.06.11.11.01	Fire Fighting Systems
1.06.11.11.02	Fire Suppression Systems
1.06.11.11.03	Lightning Protection
1.06.11.12.01	Central Control / Building Management Systems
1.06.11.13.01	Specialist Piped Supply Installation
1.06.11.13.02	Specialist Refrigeration Systems
1.06.11.13.03	Specialist Mechanical Installations
1.06.11.13.04	Specialist Electrical / Electronic Installations
1.06.11.13.05	Water Features
1.06.11.13.06	Specialist Station Equipment
1.06.11.14.01	Builder's Work in Connection with Services
1.06.12.01.01	Water Mains Supply
1.06.12.01.02	Electricity Mains Supply
1.06.12.01.03	External Transformation Devices
1.06.12.01.04	Electricity Distribution to External Plant and Equipment
1.06.12.01.05	Gas Mains Supply
1.06.12.01.06	Telecommunications and Other Communication System Connections
1.06.12.01.07	External Fuel Storage and Piped Distribution Systems
1.06.12.01.08	External Security Systems
1.06.12.01.09	External / Street Lighting Systems
1.06.12.01.10	Local / District Heating Installations
1.06.12.01.11	Builder’s Work in Connection With External Services
1.06.13.01.01	Complete Buildings
1.06.13.01.02	Building Units
1.06.13.01.03	Pods
1.06.13.01.04	Bike Stores
1.06.14.01.01	Minor Demolition Works and Alteration Works
1.06.14.02.01	Repairs to Existing Services
1.06.14.03.01	Damp-proof Course / Fungus and Beetle Eradication
1.06.14.04.01	Façade Retention
1.06.14.05.01	Cleaning Existing Surfaces
1.06.14.05.02	Protective Coatings to Existing Surfaces
1.06.14.06.01	Masonry Repairs
1.06.14.06.02	Concrete Repairs
1.06.14.06.03	Metal Repairs

1.06.14.06.04	Timber Repairs
1.06.14.06.05	Plastics Repairs
1.07.01.01.01	General excavation
1.07.01.01.02	Disposal
1.07.01.01.03	Filling
1.07.01.01.04	Filling Ancillaries
1.07.01.01.05	Grading to Profile
1.07.01.01.06	Landscaping
1.07.01.01.07	Ecology Works: state type
1.07.01.02.01	General Excavation
1.07.01.02.02	Disposal
1.07.01.02.03	Filling
1.07.01.02.04	Filling Ancillaries
1.07.01.02.05	Grading to Profile
1.07.01.02.06	Landscaping
1.07.01.02.07	Ecology Works: state type
1.07.01.03.01	General Excavation
1.07.01.03.02	Disposal
1.07.01.03.03	Filling
1.07.01.03.04	Filling Ancillaries
1.07.01.03.05	Grading to Profile
1.07.01.03.06	Landscaping
1.07.01.03.07	Ecology Works: state type
1.07.01.04.01	Permanent Monitoring
1.07.01.04.02	Removing Overburden
1.07.01.04.03	Removing Vegetation and Scaling
1.07.01.04.04	Rock Bolting and Netting
1.07.01.04.05	Soil Nailing and Ground Anchors
1.07.01.04.06	Rock or Anti-vermin Netting
1.07.02.01.01	Grouting
1.07.02.01.02	Diaphragm Walls
1.07.02.01.03	Ground Anchorages
1.07.02.02.01	Interlocking Sheet Piles
1.07.02.02.02	Rock Bolting and Netting
1.07.02.02.03	Soil Nailing and Ground Anchors
1.07.02.02.04	Rock or Anti-vermin Netting
1.07.02.03.01	Rock Filling
1.07.02.03.02	Concrete
1.07.02.03.03	Timber
1.07.02.04.01	Concrete Piles
1.07.02.04.02	Timber Piles
1.07.02.04.03	Masonry
1.07.02.04.04	Brickwork
1.07.02.04.05	Blockwork
1.07.02.04.06	Gabions
1.07.03.01.01	Tunnels: Bored
1.07.03.01.02	Tunnels: Cut and Cover
1.07.03.01.03	Adit
1.07.03.01.04	Shafts
1.07.03.01.05	Cavities
1.07.03.02.01	Masonry Lining
1.07.03.02.02	Segmental Lining
1.07.03.02.03	Applied Lining
1.07.03.02.04	Cut and Cover Tunnel Lining
1.07.03.03.01	Natural Surfaces
1.07.03.03.02	Internal Support
1.07.03.03.03	Pressure Grouting
1.07.03.03.04	Forward Probing
1.07.03.04.01	Walls: state material

1.07.03.04.02	Surface Features
1.07.03.05.01	Signs: state type
1.07.04.01.01	Subway or Underpass
1.07.04.01.02	Footings
1.07.04.02.01	Piled Foundations
1.07.04.02.02	Standard Foundations
1.07.04.02.03	Underpinning
1.07.04.03.01	In-situ Construction
1.07.04.03.02	Pre-fabricated Units
1.07.04.03.03	Piled and Faced
1.07.04.04.01	Floors
1.07.04.04.02	Roofs
1.07.04.05.01	Staircases
1.07.04.05.02	Landings and Half Landings
1.07.04.05.03	Ramps
1.07.04.05.04	Balustrading / Handrailing: state size and type
1.07.04.05.05	Access Ladders: state size and type
1.07.04.06.01	Floor
1.07.04.06.02	Walls
1.07.04.06.03	Soffit
1.07.04.06.04	Signs
1.07.04.06.05	Lighting
1.07.05.01.01	Piles / Caisson
1.07.05.01.02	Concrete Footings
1.07.05.02.01	Pier
1.07.05.02.02	Abutment
1.07.05.02.03	Wing Walls
1.07.05.02.04	Surface finishes
1.07.05.02.05	Cill Beams
1.07.05.02.06	Bridge Bearings
1.07.05.03.01	Beams
1.07.05.03.02	Structural Decking
1.07.05.03.03	Way Beam / Longitudinal Timber
1.07.05.03.04	Cable Ducts
1.07.05.04.01	Flooring
1.07.05.04.02	Ramps
1.07.05.04.03	Staircases
1.07.05.05.01	Surfacing
1.07.05.05.02	Road Marking
1.07.05.05.03	Kerbs and Channels
1.07.05.05.04	Waterproofing
1.07.05.06.01	Normal Containment Parapet
1.07.05.06.02	High Containment Parapet
1.07.05.06.03	Very High Containment Parapet
1.07.05.06.04	Ornamental / Listed Parapet
1.07.05.06.05	Balustrade
1.07.05.06.06	Parapet Handrails
1.07.05.06.07	Anti-trespass Wall / Roof
1.07.05.06.08	Suicide Cage
1.07.05.07.01	Signs
1.07.05.08.01	Pipe Work
1.07.05.08.02	Gullies with Gratings
1.07.05.08.03	Manholes and Inspection Chambers: state type
1.07.05.09.01	Excavation and Disposal
1.07.05.09.02	Filling to Structures
1.07.05.09.03	Surfacing
1.07.05.09.04	Kerbs, Channels and Edgings
1.07.06.01.01	Piles / Caisson
1.07.06.01.02	Concrete Footings

1.07.06.02.01	Pier
1.07.06.02.02	Abutment
1.07.06.02.03	Wing Walls
1.07.06.02.04	Surface Finishes
1.07.06.02.05	Cill Beams
1.07.06.02.06	Bridge Bearings
1.07.06.03.01	Beams
1.07.06.03.02	Structural Decking
1.07.06.03.03	Way Beam / Longitudinal Timber
1.07.06.03.04	Cable Ducts
1.07.06.04.01	Flooring
1.07.06.04.02	Ramps
1.07.06.04.03	Staircases
1.07.06.05.01	Surfacing
1.07.06.05.02	Road Marking
1.07.06.05.03	Kerbs and Channels
1.07.06.05.04	Waterproofing
1.07.06.06.01	Normal Containment Parapet
1.07.06.06.02	High Containment Parapet
1.07.06.06.03	Very High Containment Parapet
1.07.06.06.04	Ornamental / Listed Parapet
1.07.06.06.05	Balustrade
1.07.06.06.06	Parapet Handrails
1.07.06.06.07	Anti-trespass Wall / Roof
1.07.06.06.08	Suicide Cage
1.07.06.07.01	Signs
1.07.06.08.01	Pipe Work
1.07.06.08.02	Gullies with Gratings
1.07.06.08.03	Manholes and Inspection Chambers: state type
1.07.06.09.01	Excavation and Disposal
1.07.06.09.02	Filling to Structures
1.07.06.09.03	Surfacing
1.07.06.09.04	Kerbs, Channels and Edgings
1.07.07.01.01	Piles
1.07.07.01.02	Concrete Footings
1.07.07.01.03	Support Structure to Platforms
1.07.07.02.01	Support Structure to Platforms: state type
1.07.07.02.02	Structural Decking : state type
1.07.07.03.01	Ramps
1.07.07.03.02	Staircases
1.07.07.03.03	Access Arrangements (Ladders) to Roof / Canopies
1.07.07.03.04	Balustrading / Handrails
1.07.07.04.01	Platform Copings
1.07.07.04.02	Tactile Paving
1.07.07.04.03	Surfacing / Finishes to Platforms: state type
1.07.07.04.04	Platform Markings
1.07.07.05.01	Support Structure to Roof / Canopy: state type
1.07.07.05.02	Coverings
1.07.07.06.01	Signs / Notices
1.07.07.06.02	Seating
1.07.07.07.01	Pipework Above Ground: state type and size
1.07.07.07.02	Pipework Below Ground: state type and size
1.07.07.07.03	Cable Ducts
1.07.07.07.04	Manholes, Catchpits, Turning Chambers and other Inspection Pits: state type and size
1.07.08.01.01	Foundations: Linear
1.07.08.01.02	Foundations: Isolated
1.07.08.01.03	Piling
1.07.08.01.04	Filling
1.07.08.02.01	Walls: Gravity Type

1.07.08.02.02	Walls: Cantilever
1.07.08.02.03	Walls: King Post Construction
1.07.08.02.04	Walls: Piled Construction
1.07.08.02.05	Surface Feature
1.07.08.02.06	Interlocking Sheet Piles
1.07.08.02.07	Waterproof Membranes
1.07.08.02.08	Gabions
1.07.08.02.09	Drain Hole or Weep Hole
1.07.09.01.01	Fences: state type
1.07.09.01.02	Gates: Personnel
1.07.09.01.03	Gates: Vehicular
1.07.09.01.04	Stiles: state type
1.07.09.01.05	Avalanche Fencing
1.07.09.01.06	Catch Walls: state type
1.07.09.01.07	Take Down and Dispose of Fencing: state size and type
1.07.09.01.08	Take Down and Dispose of Gates and Stiles: state size and type
1.07.09.02.01	Fixed Barriers
1.07.09.02.02	Access Barriers: Personnel
1.07.09.02.03	Access Barriers: Vehicular
1.07.09.02.04	Take Down and Dispose of Vehicular Barriers: state type
1.07.09.02.05	Take Down and Dispose of Pedestrian Guard Rails : state type
1.07.10.01.01	Drain Pipes and Trenches: state size and depth
1.07.10.01.02	Channels and Gratings
1.07.10.01.03	Gullies
1.07.10.01.04	Manholes and Inspection Chambers: state type
1.07.10.01.05	Interceptors
1.07.10.01.06	Connections to Public Mains Drainage
1.07.10.02.01	Drain Pipes and Trenches: state size and depth
1.07.10.02.02	Channels and Gratings
1.07.10.02.03	Gullies
1.07.10.02.04	Manholes and Inspection Chambers: state type
1.07.10.02.05	Connections to Public Mains Drainage
1.07.10.03.01	Drain Pipes and Trenches: state size and depth
1.07.10.03.02	Drain Pipes and Supports Above Ground: state size and support type / spacings
1.07.10.03.03	Channels and Gratings: state type and size
1.07.10.03.04	Manholes and Inspection Chambers: state size and type
1.07.10.03.05	Storage Tanks: state type and size
1.07.10.04.01	Ponds: Excavation and Disposal
1.07.10.04.02	Watercourses: Excavation and Disposal
1.07.10.04.03	Linings: Balancing Ponds
1.07.10.04.04	Linings: Watercourses
1.07.10.05.01	French Drains: state pipes and filling
1.07.10.05.02	Lined Ditches
1.07.10.05.03	Soakaways
1.07.10.05.04	Outfalls Including Fittings
1.07.10.06.01	New Culverts: state type
1.07.10.06.02	Existing Culverts: Lining
1.07.10.07.01	Testing: During the Progress of the Works
1.07.10.07.02	Testing : On Completion of the Works
1.07.10.07.03	Commissioning: Work Completed in Sections
1.07.10.07.04	Commissioning: Co-Ordination of Sectional Work
1.07.10.07.05	Commissioning and Handover
1.07.10.08.01	Excavation and Disposal of Buried Pipe Drainage: state type and depth
1.07.10.08.02	Take Up and Dispose Culverts: state type and size
1.07.10.08.03	Remove Manholes and Inspection Chambers: state size and type
1.07.10.08.04	Take Up and Dispose of Gullies and Fill Void
1.07.11.01.01	Excavation and Disposal
1.07.11.01.02	Filling to Structures
1.07.11.01.03	Blanket and Geotextile Layer

1.07.11.01.04	Excavation and Disposal of Track Foundation Materials : state type
1.07.11.02.01	Excavation and Disposal
1.07.11.02.02	Filling to Structures
1.07.11.02.03	Blanket and Geotextile Layer
1.07.11.02.04	Excavation and Disposal of Track Foundation Materials : state type
1.07.12.01.01	Excavation and Disposal
1.07.12.01.02	Filling to Structures
1.07.12.01.03	Surfaced Access Ways: Vehicular
1.07.12.01.04	Surfaced Access Ways: Pedestrian
1.07.12.01.05	Surfacing to Ducting or Troughing: Paved Finish
1.07.12.01.06	Kerbs, Channels and Edgings
1.07.12.02.01	Excavation and Disposal
1.07.12.02.02	Filling to Structures
1.07.12.02.03	Surfaced Access Ways: Vehicular
1.07.12.02.04	Surfaced Access Ways: Pedestrian
1.07.12.02.05	Surfacing to Ducting or Troughing: Paved Finish
1.07.12.02.06	Kerbs, Channels and Edgings
1.07.12.03.01	Excavation and Disposal
1.07.12.03.02	Filling to Structures
1.07.12.03.03	Surfaced Access Ways: Vehicular
1.07.12.03.04	Surfaced Access Ways: Pedestrian
1.07.12.03.05	Surfacing to Ducting or Troughing: Paved Finish
1.07.12.03.06	Kerbs, Channels and Edgings
1.07.12.04.01	Excavation and Disposal
1.07.12.04.02	Filling to Structures
1.07.12.04.03	Surfaced Access Ways: Vehicular
1.07.12.04.04	Surfaced Access Ways: Pedestrian
1.07.12.04.05	Surfacing to Ducting or Troughing: Paved Finish
1.07.12.04.06	Kerbs, Channels and Edgings
1.07.12.05.01	Cable Routes: state type
1.07.12.05.02	Service Ducts: state details
1.07.12.07.01	Site / Street Furniture: state type
1.07.12.07.02	Ornamental Features: state type
1.07.12.08.01	Break Up and Dispose of Surfacing and Paving
1.07.12.08.02	Take Up and Dispose of Kerbs, Edgings and Associated Concrete Backing: state type
1.07.12.08.03	Take Up and Recover Lighting Cable Routes and Ducts: state type and size
1.07.12.08.04	Take Up and Recover Light Fittings : state type and size
1.07.12.08.05	Take Up and Recover Other Street Furniture: state type and size
1.07.13.01.01	Seeding and Turfing
1.07.13.01.02	External Planting: state type
1.07.13.01.03	Irrigation Systems: state type
1.07.13.02.01	Ecology Works: state type
1.07.14.01.01	Traditional Concrete Troughing
1.07.14.01.02	Concrete Based Troughing
1.07.14.01.03	Non-cementitious Troughing
1.07.14.01.04	Transition Unit
1.07.14.01.05	T' Piece
1.07.14.01.06	De-lid and Lid Existing Troughing to Receive Cables
1.07.14.01.07	Abandonment and Recovery of Containment and Trough Route: state type
1.07.14.02.01	Traditional Concrete Troughing
1.07.14.02.02	Concrete Based Troughing
1.07.14.02.03	Non-cementitious Troughing
1.07.14.02.04	Transition Unit
1.07.14.02.05	T' Piece
1.07.14.02.06	De-lid and Lid Existing Troughing to Receive Cables
1.07.14.02.07	Abandonment and Recovery of Containment and Trough Route: state type
1.07.14.03.01	Traditional Concrete Troughing
1.07.14.03.02	Concrete Based Troughing
1.07.14.03.03	Non-cementitious Troughing

1.07.14.03.04	Transition Unit
1.07.14.03.05	T' Piece
1.07.14.03.06	De-lid and Lid Existing Troughing to Receive Cables
1.07.14.03.07	Abandonment and Recovery of Containment and Trough Route: state type
1.07.15.01.01	Ducts: state type
1.07.15.01.02	Draw pits and Chambers: state type
1.07.15.01.03	Cable Bridge: state type
1.07.15.02.01	Ducts: state type
1.07.15.02.02	Draw pits and Chambers: state type
1.07.15.02.03	Cable Bridge: state type
1.07.15.03.01	Ducts: state type
1.07.15.03.02	Draw pits and Chambers: state type
1.07.15.03.03	Cable Bridge: state type
1.07.15.04.01	Ducts: state type
1.07.15.04.02	Draw pits and Chambers: state type
1.07.15.04.03	Cable Bridge: state type
1.07.15.05.01	Ducts: state type
1.07.15.05.02	Draw pits and Chambers: state type
1.07.15.05.03	Cable Bridge: state type
1.08.01.01.01	Physical Archaeological Investigation
1.08.01.01.02	Attendance on Archaeologist
1.08.01.02.01	Trapping and Relocation of Species
1.08.01.02.02	Temporary Fences and/or Barriers
1.08.01.03.01	Unexploded Munitions or Other
1.08.01.03.02	Ordnance Other Investigations: State Component Cost Item
1.08.02.01.01	General Clearance
1.08.02.01.02	Clearance of Vegetation
1.08.02.01.03	Surveys
1.08.02.01.04	Management of Shrubs, Bushes and Trees
1.08.02.02.01	Toxic and / or Hazardous Parts of Building Fabric
1.08.02.02.02	Toxic and / or Hazardous Components from Service Installations
1.08.02.03.01	Contaminated Ground: Removal
1.08.02.03.02	Contaminated Ground: Treatment
1.08.02.04.01	Invasive Plant Growth: Removal
1.08.02.04.02	Invasive Plant Growth: Treatment
1.08.02.05.01	Site De-watering and Pumping
1.08.02.05.02	Soil Stabilisation
1.08.02.05.03	Ground Gas Ventilation
1.08.02.05.04	Compaction
1.08.02.05.05	Compensation Grouting
1.08.02.06.01	Diversions and Interruptions
1.08.02.06.02	Hardstanding's
1.08.02.06.03	Bridges and Walkways
1.08.03.01.01	Demolition: Entire Structures
1.08.03.01.02	Demolition: Partial Structures
1.08.03.01.03	Retention of Structures
1.08.03.02.01	Underbridges
1.08.03.02.02	Overbridges
1.08.03.02.03	Tunnels
1.08.03.02.04	Platforms
1.08.03.02.05	Cables and Containment
1.08.03.03.01	Permanent Way: Removal and Reinstatement
1.08.03.03.02	Railway Control System Equipment Removal and Reinstatement
1.08.03.03.03	Level Crossings
1.08.03.03.04	Overhead Line Equipment (OLE) Systems: Removal and Reinstatement
1.08.03.03.05	Telecommunication Equipment: Removal and Reinstatement
1.08.03.03.06	Platform and Building Furniture and Equipment: Removal and Reinstatement
1.08.03.03.07	Cables and Containment: Removal and Reinstatement
1.08.03.03.08	Boundary Fencing and Enclosures: Removal and Reinstatement

1.09.01.01.01	Shell: including Painting
1.09.01.01.02	Interior Fit Out and Finishes: including Doors
1.09.01.01.03	Glazing / Windows
1.09.01.01.04	Bogies
1.09.01.01.05	Braking
1.09.01.01.06	Articulation
1.09.01.01.07	Traction Motors
1.09.01.01.08	Coupling
1.09.01.01.09	Control and Communications
1.09.01.01.10	Auxiliary Equipment and Batteries
1.09.01.01.11	Heating, Ventilation and Air Conditioning
1.09.01.01.12	Driver's Console and Cab Equipment
1.09.01.02.01	Shell: including Painting
1.09.01.02.02	Interior Fit Out and Finishes: including Doors
1.09.01.02.03	Glazing / Windows
1.09.01.02.04	Bogies
1.09.01.02.05	Braking
1.09.01.02.06	Articulation
1.09.01.02.07	Traction Motors
1.09.01.02.08	Coupling
1.09.01.02.09	Control and Communications
1.09.01.02.10	Auxiliary Equipment and Batteries
1.09.01.02.11	Heating, Ventilation and Air Conditioning
1.09.01.03.01	Shell: including Painting
1.09.01.03.02	Interior Fit Out and Finishes: including Doors
1.09.01.03.03	Glazing / Windows
1.09.01.03.04	Bogies
1.09.01.03.05	Braking
1.09.01.03.06	Articulation
1.09.01.03.07	Traction Motors
1.09.01.03.08	Coupling
1.09.01.03.09	Control and Communications
1.09.01.03.10	Auxiliary Equipment and Batteries
1.09.01.03.11	Heating, Ventilation and Air Conditioning
1.09.02.01.01	Shell: including Painting
1.09.02.01.02	Interior Fit Out and Finishes: including Doors
1.09.02.01.03	Glazing / Windows
1.09.02.01.04	Bogies
1.09.02.01.05	Braking
1.09.02.01.06	Articulation
1.09.02.01.07	Traction Motors
1.09.02.01.08	Coupling
1.09.02.01.09	Control and Communications
1.09.02.01.10	Auxiliary Equipment and Batteries
1.09.02.01.11	Heating, Ventilation and Air Conditioning
1.09.02.01.12	Driver's Console and Cab Equipment
1.09.03.01.01	Shell: including Painting
1.09.03.01.02	Interior Fit Out and Finishes: including Doors
1.09.03.01.03	Glazing / Windows
1.09.03.01.04	Bogies
1.09.03.01.05	Braking
1.09.03.01.06	Articulation
1.09.03.01.07	Traction Motors
1.09.03.01.08	Coupling
1.09.03.01.09	Control and Communications
1.09.03.01.10	Auxiliary Equipment and Batteries
1.09.03.01.11	Heating, Ventilation and Air Conditioning
1.09.03.01.12	Driver's Console and Cab Equipment
1.09.04.01.01	Shell: including Painting

1.09.04.01.02	Interior Fit Out and Finishes: including Doors
1.09.04.01.03	Glazing / Windows
1.09.04.01.04	Bogies
1.09.04.01.05	Braking
1.09.04.01.06	Articulation
1.09.04.01.07	Traction Motors
1.09.04.01.08	Coupling
1.09.04.01.09	Control and Communications
1.09.04.01.10	Auxiliary Equipment and Batteries
1.09.04.01.11	Heating, Ventilation and Air Conditioning
1.09.04.01.12	Driver's Console and Cab Equipment
1.09.05.01.01	Fit of Signalling Equipment: Supplier and European Traffic Management Requirements
1.09.06.01.01	Pre-delivery Testing
1.09.06.01.02	Post-delivery Testing
1.09.06.02.01	Commissioning
1.09.06.02.02	Handover
1.09.07.01.01	Initial Spares
1.09.07.01.02	Maintenance Spares
1.09.07.02.01	Service Agreement
1.09.07.02.02	Third Party Maintenance

Level 1	Level 2	Level 3	Level 4	Item
1.01				**Railway Control Systems**
1.01	1.01.01			**Signalling Systems**
1.01	1.01.01	1.01.01.01		**Controls and Monitoring Systems**
1.01	1.01.01	1.01.01.01	1.01.01.01.01	Consoles and Panels
1.01	1.01.01	1.01.01.01	1.01.01.01.02	Lever Frames
1.01	1.01.01	1.01.01.01	1.01.01.01.03	Ground Frames
1.01	1.01.01	1.01.01.01	1.01.01.01.04	Train Describers
1.01	1.01.01	1.01.01.01	1.01.01.01.05	Supervisory Systems
1.01	1.01.01	1.01.01.01	1.01.01.01.06	Signalling Simulator
1.01	1.01.01	1.01.01.02		**Interlocking**
1.01	1.01.01	1.01.01.02	1.01.01.02.01	Micro-processor Based Systems
1.01	1.01.01	1.01.01.02	1.01.01.02.02	Electro-mechanical Interlocking
1.01	1.01.01	1.01.01.02	1.01.01.02.03	Mechanical
1.01	1.01.01	1.01.01.02	1.01.01.02.04	Trackside Interlocking Interface Unit
1.01	1.01.01	1.01.01.02	1.01.01.02.05	Tokenless Block
1.01	1.01.01	1.01.01.03		**Points Mechanisms**
1.01	1.01.01	1.01.01.03	1.01.01.03.01	Electrical
1.01	1.01.01	1.01.01.03	1.01.01.03.02	Hydraulic
1.01	1.01.01	1.01.01.03	1.01.01.03.03	Electro-pneumatic
1.01	1.01.01	1.01.01.03	1.01.01.03.04	Air
1.01	1.01.01	1.01.01.03	1.01.01.03.05	Mechanical
1.01	1.01.01	1.01.01.04		**Signals and Indicators**
1.01	1.01.01	1.01.01.04	1.01.01.04.01	Colour light signal
1.01	1.01.01	1.01.01.04	1.01.01.04.02	Banner Repeaters
1.01	1.01.01	1.01.01.04	1.01.01.04.03	Position Light Signal
1.01	1.01.01	1.01.01.04	1.01.01.04.04	Route Indicators
1.01	1.01.01	1.01.01.04	1.01.01.04.05	Signal Functions
1.01	1.01.01	1.01.01.04	1.01.01.04.06	Mechanical Signal
1.01	1.01.01	1.01.01.04	1.01.01.04.07	Operational Signs and Noticeboards
1.01	1.01.01	1.01.01.04	1.01.01.04.08	Other
1.01	1.01.01	1.01.01.05		**Train Detection Systems**
1.01	1.01.01	1.01.01.05	1.01.01.05.01	Track Circuits
1.01	1.01.01	1.01.01.05	1.01.01.05.02	Axle Counters
1.01	1.01.01	1.01.01.05	1.01.01.05.03	Treadles
1.01	1.01.01	1.01.01.05	1.01.01.05.04	Balise
1.01	1.01.01	1.01.01.05	1.01.01.05.05	Insulated Block Joints (IBJs)
1.01	1.01.01	1.01.01.05	1.01.01.05.06	Impedance Bonds
1.01	1.01.01	1.01.01.05	1.01.01.05.07	Hot Axle Box Detectors
1.01	1.01.01	1.01.01.06		**Train Protection Systems**
1.01	1.01.01	1.01.01.06	1.01.01.06.01	Automatic Warning System (AWS)
1.01	1.01.01	1.01.01.06	1.01.01.06.02	Train Protection Warning System (TPWS)
1.01	1.01.01	1.01.01.06	1.01.01.06.03	Automatic Train Control (ATC)
1.01	1.01.01	1.01.01.06	1.01.01.06.04	Automatic Train Protection (ATP)
1.01	1.01.01	1.01.01.07		**Remote Control Systems**
1.01	1.01.01	1.01.01.07	1.01.01.07.01	Time Division Data Transmission Systems (TDM)
1.01	1.01.01	1.01.01.07	1.01.01.07.02	Frequency Division Data Transmission Systems (FDM)
1.01	1.01.01	1.01.01.07	1.01.01.07.03	Radio Electronic Tokenless Block (RETB)
1.01	1.01.01	1.01.01.07	1.01.01.07.04	Lockout Device (PLOD)
1.01	1.01.01	1.01.01.07	1.01.01.07.05	Alarms, Warnings and Controls
1.01	1.01.01	1.01.01.07	1.01.01.07.06	Other; state type
1.01	1.01.01	1.01.01.08		**Cables and Containment**
1.01	1.01.01	1.01.01.08	1.01.01.08.01	Cables
1.01	1.01.01	1.01.01.08	1.01.01.08.02	Containment in Buildings or Structures

1.01	1.01.01	1.01.01.08	1.01.01.08.03	Tremble Devices / Theft Protection
1.01	1.01.01	1.01.01.09		**Signal Support Structures and Foundations**
1.01	1.01.01	1.01.01.09	1.01.01.09.01	Freestanding Single Post: Straight
1.01	1.01.01	1.01.01.09	1.01.01.09.02	Freestanding Single Post: Cranked
1.01	1.01.01	1.01.01.09	1.01.01.09.03	Freestanding Single Post: Lightweight
1.01	1.01.01	1.01.01.09	1.01.01.09.04	Freestanding Single Post: Collapsible
1.01	1.01.01	1.01.01.09	1.01.01.09.05	Fitting; Wall or Roof: state type
1.01	1.01.01	1.01.01.09	1.01.01.09.06	Structural Ancillaries, Fitting to Existing Structures
1.01	1.01.01	1.01.01.09	1.01.01.09.07	Signal Support Structure: Cantilever Single Track
1.01	1.01.01	1.01.01.09	1.01.01.09.08	Signal Support Structure: Cantilever Over 2 Tracks
1.01	1.01.01	1.01.01.09	1.01.01.09.09	Signal Support Structure: Cantilever Over 3 Tracks
1.01	1.01.01	1.01.01.09	1.01.01.09.10	Signal Support Structure: Cantilever Over 4 Tracks
1.01	1.01.01	1.01.01.09	1.01.01.09.11	Signal Support Structure: Gantry / Portal 2 Tracks
1.01	1.01.01	1.01.01.09	1.01.01.09.12	Signal Support Structure: Gantry / Portal 3 Tracks
1.01	1.01.01	1.01.01.09	1.01.01.09.13	Signal Support Structure: Gantry / Portal 4 Tracks
1.01	1.01.01	1.01.01.09	1.01.01.09.14	Signal Support Structure: Gantry / Portal 5 Tracks
1.01	1.01.01	1.01.01.09	1.01.01.09.15	Signal Support Structure: Gantry / Portal 6 Tracks
1.01	1.01.01	1.01.01.09	1.01.01.09.16	Signal Support Structure: Gantry / Portal 7 Tracks
1.01	1.01.01	1.01.01.09	1.01.01.09.17	Signal Support Structure: Gantry / Portal 8 Tracks
1.01	1.01.01	1.01.01.09	1.01.01.09.18	Signal Support Structure: Gantry / Portal 9 Tracks
1.01	1.01.01	1.01.01.09	1.01.01.09.19	Signal Support Structure: Gantry / Portal 10 Tracks
1.01	1.01.01	1.01.01.09	1.01.01.09.20	Immunisation
1.01	1.01.01	1.01.01.10		**Equipment Housings, Platforms and Foundations**
1.01	1.01.01	1.01.01.10	1.01.01.10.01	Location Case complete with Racking and Equipment: state type
1.01	1.01.01	1.01.01.10	1.01.01.10.02	Portable Building complete with Services
1.01	1.01.01	1.01.01.10	1.01.01.10.03	Trackside Equipment: Level Ground: state type foundation
1.01	1.01.01	1.01.01.10	1.01.01.10.04	Trackside Equipment: Staging: 'Up Bank' for Cut and 'Down Bank' for E
1.01	1.01.01	1.01.01.11		**Stage Works**
1.01	1.01.01	1.01.01.11	1.01.01.11.01	Stage : state reference
1.01	1.01.01	1.01.01.12		**Fringe : state location**
1.01	1.01.01	1.01.01.12	1.01.01.12.01	Fringe : state reference
1.01	1.01.01	1.01.01.13		**Level Crossings: state type and location**
1.01	1.01.01	1.01.01.13	1.01.01.13.01	Highway Works
1.01	1.01.01	1.01.01.13	1.01.01.13.02	Barriers
1.01	1.01.01	1.01.01.13	1.01.01.13.03	Signal and Traffic Protection
1.01	1.01.01	1.01.01.13	1.01.01.13.04	Controls and Operating Systems: state type
1.01	1.01.01	1.01.01.14		**Testing and Commissioning**
1.01	1.01.01	1.01.01.14	1.01.01.14.01	Testing
1.01	1.01.01	1.01.01.14	1.01.01.14.02	Commissioning and Handover
1.01	1.01.01	1.01.01.15		**Strategic Spares**
1.01	1.01.01	1.01.01.15	1.01.01.15.01	Spares: state type
1.01	1.01.01	1.01.01.16		**Abandonment, Recovery and Disposal of Redundant Equipment**
1.01	1.01.01	1.01.01.16	1.01.01.16.01	Materials and Equipment
1.01	1.01.02			**Traffic Management Systems (Non-digital)**
1.01	1.01.02	1.01.02.01		**Traffic Management Systems (Non-digital)**
1.01	1.01.02	1.01.02.01	1.01.02.01.01	Supervisory Control
1.01	1.01.02	1.01.02.01	1.01.02.01.02	Incident Management Systems (IMS)
1.01	1.01.02	1.01.02.01	1.01.02.01.03	Stock and Crew Systems
1.01	1.01.02	1.01.02.01	1.01.02.01.04	Safe Track Worker Access
1.01	1.01.02	1.01.02.01	1.01.02.01.05	Other
1.01	1.01.03			**Digital Control Systems: Traffic Management (TM)**
1.01	1.01.03	1.01.03.01		**Contractor Designed System: Traffic Management System (TM)**
1.01	1.01.03	1.01.03.01	1.01.03.01.01	Hardware
1.01	1.01.03	1.01.03.01	1.01.03.01.02	Installation

1.01	1.01.03	1.01.03.01	1.01.03.01.03	Computer Software and System Development
1.01	1.01.03	1.01.03.02		**Testing and Commissioning**
1.01	1.01.03	1.01.03.02	1.01.03.02.01	Testing
1.01	1.01.03	1.01.03.02	1.01.03.02.02	Commissioning and Handover
1.01	1.01.04			**Digital Control Systems: European Train Control System (ETCS)**
1.01	1.01.04	1.01.04.01		**Contractor Designed System: ETCS**
1.01	1.01.04	1.01.04.01	1.01.04.01.01	Hardware
1.01	1.01.04	1.01.04.01	1.01.04.01.02	Installation
1.01	1.01.04	1.01.04.01	1.01.04.01.03	Computer Software and System Development
1.01	1.01.04	1.01.04.02		**Remote Control Systems**
1.01	1.01.04	1.01.04.02	1.01.04.02.01	Radio Block Control (RBC)
1.01	1.01.04	1.01.04.03		**Testing and Commissioning**
1.01	1.01.04	1.01.04.03	1.01.04.03.01	Testing
1.01	1.01.04	1.01.04.03	1.01.04.03.02	Commissioning and Handover
1.01	1.01.05			**Other Digital Systems**
1.01	1.01.05	1.01.05.01		**Contractor Designed System: CDAS**
1.01	1.01.05	1.01.05.01	1.01.05.01.01	Hardware
1.01	1.01.05	1.01.05.01	1.01.05.01.02	Installation
1.01	1.01.05	1.01.05.01	1.01.05.01.03	Computer Software and System Development
1.01	1.01.05	1.01.05.02		**Contractor Designed System: ATO GoA 1 and 2**
1.01	1.01.05	1.01.05.02	1.01.05.02.01	Hardware
1.01	1.01.05	1.01.05.02	1.01.05.02.02	Installation
1.01	1.01.05	1.01.05.02	1.01.05.02.03	Computer Software and System Development
1.01	1.01.05	1.01.05.03		**Contractor Designed System: ATO GoA 3**
1.01	1.01.05	1.01.05.03	1.01.05.03.01	Hardware
1.01	1.01.05	1.01.05.03	1.01.05.03.02	Installation
1.01	1.01.05	1.01.05.03	1.01.05.03.03	Computer Software and System Development
1.01	1.01.05	1.01.05.04		**Contractor Designed System: ATO Goal 4**
1.01	1.01.05	1.01.05.04	1.01.05.04.01	Hardware
1.01	1.01.05	1.01.05.04	1.01.05.04.02	Installation
1.01	1.01.05	1.01.05.04	1.01.05.04.03	Computer Software and System Development
1.01	1.01.05	1.01.05.05		**Contractor Designed System: CIS (Information System)**
1.01	1.01.05	1.01.05.05	1.01.05.05.01	Hardware
1.01	1.01.05	1.01.05.05	1.01.05.05.02	Installation
1.01	1.01.05	1.01.05.05	1.01.05.05.03	Computer Software and System Development
1.01	1.01.05	1.01.05.06		**Contractor Designed System: Stock and Crew Systems**
1.01	1.01.05	1.01.05.06	1.01.05.06.01	Hardware
1.01	1.01.05	1.01.05.06	1.01.05.06.02	Installation
1.01	1.01.05	1.01.05.06	1.01.05.06.03	Computer Software and System Development
1.01	1.01.05	1.01.05.07		**Contractor Designed System: Incident Management System**
1.01	1.01.05	1.01.05.07	1.01.05.07.01	Hardware
1.01	1.01.05	1.01.05.07	1.01.05.07.02	Installation
1.01	1.01.05	1.01.05.07	1.01.05.07.03	Computer Software & System Development
1.01	1.01.05	1.01.05.08		**Other Contractor Designed Digital System: state type**
1.01	1.01.05	1.01.05.08	1.01.05.08.01	Hardware
1.01	1.01.05	1.01.05.08	1.01.05.08.02	Installation
1.01	1.01.05	1.01.05.08	1.01.05.08.03	Computer Software and System Development

Level 1	Level 2	Level 3	Level 4	Item
1.02				**Train Power Systems**
1.02	1.02.01			**Power Distribution**
1.02	1.02.01	1.02.01.01		**Auto Transformer Site (ATS)**
1.02	1.02.01	1.02.01.01	1.02.01.01.01	Base
1.02	1.02.01	1.02.01.01	1.02.01.01.02	Enclosure
1.02	1.02.01	1.02.01.01	1.02.01.01.03	Compound
1.02	1.02.01	1.02.01.01	1.02.01.01.04	Site Access
1.02	1.02.01	1.02.01.01	1.02.01.01.05	Switchgear Equipment
1.02	1.02.01	1.02.01.01	1.02.01.01.06	Transformers
1.02	1.02.01	1.02.01.01	1.02.01.01.07	Rectifiers
1.02	1.02.01	1.02.01.01	1.02.01.01.08	Protection and Control Equipment
1.02	1.02.01	1.02.01.01	1.02.01.01.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.02	1.02.01	1.02.01.01	1.02.01.01.10	Data Connection to Control Centre
1.02	1.02.01	1.02.01.02		**Auto Transformer Feeder Site (ATFS)**
1.02	1.02.01	1.02.01.02	1.02.01.02.01	Base
1.02	1.02.01	1.02.01.02	1.02.01.02.02	Enclosure
1.02	1.02.01	1.02.01.02	1.02.01.02.03	Compound
1.02	1.02.01	1.02.01.02	1.02.01.02.04	Site Access
1.02	1.02.01	1.02.01.02	1.02.01.02.05	Switchgear Equipment
1.02	1.02.01	1.02.01.02	1.02.01.02.06	Transformers
1.02	1.02.01	1.02.01.02	1.02.01.02.07	Rectifiers
1.02	1.02.01	1.02.01.02	1.02.01.02.08	Protection and Control Equipment
1.02	1.02.01	1.02.01.02	1.02.01.02.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.02	1.02.01	1.02.01.02	1.02.01.02.10	Data Connection to Control Centre
1.02	1.02.01	1.02.01.03		**Mid Point Auto Transformer Site (MPATS)**
1.02	1.02.01	1.02.01.03	1.02.01.03.01	Base
1.02	1.02.01	1.02.01.03	1.02.01.03.02	Enclosure
1.02	1.02.01	1.02.01.03	1.02.01.03.03	Compound
1.02	1.02.01	1.02.01.03	1.02.01.03.04	Site Access
1.02	1.02.01	1.02.01.03	1.02.01.03.05	Switchgear Equipment
1.02	1.02.01	1.02.01.03	1.02.01.03.06	Transformers
1.02	1.02.01	1.02.01.03	1.02.01.03.07	Rectifiers
1.02	1.02.01	1.02.01.03	1.02.01.03.08	Protection and Control Equipment
1.02	1.02.01	1.02.01.03	1.02.01.03.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.02	1.02.01	1.02.01.03	1.02.01.03.10	Data Connection to Control Centre
1.02	1.02.01	1.02.01.04		**Sectioning Auto Transformer Site(SATS)**
1.02	1.02.01	1.02.01.04	1.02.01.04.01	Base
1.02	1.02.01	1.02.01.04	1.02.01.04.02	Enclosure
1.02	1.02.01	1.02.01.04	1.02.01.04.03	Compound
1.02	1.02.01	1.02.01.04	1.02.01.04.04	Site Access
1.02	1.02.01	1.02.01.04	1.02.01.04.05	Switchgear Equipment
1.02	1.02.01	1.02.01.04	1.02.01.04.06	Transformers
1.02	1.02.01	1.02.01.04	1.02.01.04.07	Rectifiers
1.02	1.02.01	1.02.01.04	1.02.01.04.08	Protection and Control Equipment
1.02	1.02.01	1.02.01.04	1.02.01.04.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.02	1.02.01	1.02.01.04	1.02.01.04.10	Data Connection to Control Centre
1.02	1.02.01	1.02.01.05		**Main Grid Traction Supply Substation (Feeder Station)**
1.02	1.02.01	1.02.01.05	1.02.01.05.01	Base
1.02	1.02.01	1.02.01.05	1.02.01.05.02	Enclosure
1.02	1.02.01	1.02.01.05	1.02.01.05.03	Compound
1.02	1.02.01	1.02.01.05	1.02.01.05.04	Site Access

1.02	1.02.01	1.02.01.05	1.02.01.05.05	Switchgear Equipment
1.02	1.02.01	1.02.01.05	1.02.01.05.06	Transformers
1.02	1.02.01	1.02.01.05	1.02.01.05.07	Rectifiers
1.02	1.02.01	1.02.01.05	1.02.01.05.08	Protection and Control Equipment
1.02	1.02.01	1.02.01.05	1.02.01.05.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.02	1.02.01	1.02.01.05	1.02.01.05.10	Data Connection to Control Centre
1.02	1.02.01	1.02.01.06		**Track Sectioning Switch (TSS)**
1.02	1.02.01	1.02.01.06	1.02.01.06.01	Base
1.02	1.02.01	1.02.01.06	1.02.01.06.02	Enclosure
1.02	1.02.01	1.02.01.06	1.02.01.06.03	Compound
1.02	1.02.01	1.02.01.06	1.02.01.06.04	Site Access
1.02	1.02.01	1.02.01.06	1.02.01.06.05	Switchgear Equipment
1.02	1.02.01	1.02.01.06	1.02.01.06.06	Transformers
1.02	1.02.01	1.02.01.06	1.02.01.06.07	Rectifiers
1.02	1.02.01	1.02.01.06	1.02.01.06.08	Protection and Control Equipment
1.02	1.02.01	1.02.01.06	1.02.01.06.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.02	1.02.01	1.02.01.06	1.02.01.06.10	Data Connection to Control Centre
1.02	1.02.01	1.02.01.07		**DC Substation**
1.02	1.02.01	1.02.01.07	1.02.01.07.01	Base
1.02	1.02.01	1.02.01.07	1.02.01.07.02	Enclosure
1.02	1.02.01	1.02.01.07	1.02.01.07.03	Compound
1.02	1.02.01	1.02.01.07	1.02.01.07.04	Site Access
1.02	1.02.01	1.02.01.07	1.02.01.07.05	Switchgear Equipment
1.02	1.02.01	1.02.01.07	1.02.01.07.06	Transformers
1.02	1.02.01	1.02.01.07	1.02.01.07.07	Rectifiers
1.02	1.02.01	1.02.01.07	1.02.01.07.08	Protection and Control Equipment
1.02	1.02.01	1.02.01.07	1.02.01.07.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.02	1.02.01	1.02.01.07	1.02.01.07.10	Data Connection to Control Centre
1.02	1.02.01	1.02.01.08		**Track Paralleling Hut**
1.02	1.02.01	1.02.01.08	1.02.01.08.01	Base
1.02	1.02.01	1.02.01.08	1.02.01.08.02	Enclosure
1.02	1.02.01	1.02.01.08	1.02.01.08.03	Compound
1.02	1.02.01	1.02.01.08	1.02.01.08.04	Site Access
1.02	1.02.01	1.02.01.08	1.02.01.08.05	Switchgear Equipment
1.02	1.02.01	1.02.01.08	1.02.01.08.06	Transformers
1.02	1.02.01	1.02.01.08	1.02.01.08.07	Rectifiers
1.02	1.02.01	1.02.01.08	1.02.01.08.08	Protection and Control Equipment
1.02	1.02.01	1.02.01.08	1.02.01.08.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.02	1.02.01	1.02.01.08	1.02.01.08.10	Data Connection to Control Centre
1.02	1.02.01	1.02.01.09		**Structure Mounted Outdoor Switchgear (SMOS)**
1.02	1.02.01	1.02.01.09	1.02.01.09.01	Base
1.02	1.02.01	1.02.01.09	1.02.01.09.02	Enclosure
1.02	1.02.01	1.02.01.09	1.02.01.09.03	Compound
1.02	1.02.01	1.02.01.09	1.02.01.09.04	Site Access
1.02	1.02.01	1.02.01.09	1.02.01.09.05	Switchgear Equipment
1.02	1.02.01	1.02.01.09	1.02.01.09.06	Transformers
1.02	1.02.01	1.02.01.09	1.02.01.09.07	Rectifiers
1.02	1.02.01	1.02.01.09	1.02.01.09.08	Protection and Control Equipment
1.02	1.02.01	1.02.01.09	1.02.01.09.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.02	1.02.01	1.02.01.09	1.02.01.09.10	Data Connection to Control Centre
1.02	1.02.01	1.02.01.10		**Containerised Switchgear**
1.02	1.02.01	1.02.01.10	1.02.01.10.01	Base

1.02	1.02.01	1.02.01.10	1.02.01.10.02	Enclosure
1.02	1.02.01	1.02.01.10	1.02.01.10.03	Compound
1.02	1.02.01	1.02.01.10	1.02.01.10.04	Site Access
1.02	1.02.01	1.02.01.10	1.02.01.10.05	Switchgear Equipment
1.02	1.02.01	1.02.01.10	1.02.01.10.06	Transformers
1.02	1.02.01	1.02.01.10	1.02.01.10.07	Rectifiers
1.02	1.02.01	1.02.01.10	1.02.01.10.08	Protection and Control Equipment
1.02	1.02.01	1.02.01.10	1.02.01.10.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.02	1.02.01	1.02.01.10	1.02.01.10.10	Data Connection to Control Centre
1.02	1.02.01	1.02.01.11		**Booster Transformer**
1.02	1.02.01	1.02.01.11	1.02.01.11.01	Base
1.02	1.02.01	1.02.01.11	1.02.01.11.02	Enclosure
1.02	1.02.01	1.02.01.11	1.02.01.11.03	Compound
1.02	1.02.01	1.02.01.11	1.02.01.11.04	Site Access
1.02	1.02.01	1.02.01.11	1.02.01.11.05	Switchgear Equipment
1.02	1.02.01	1.02.01.11	1.02.01.11.06	Transformers
1.02	1.02.01	1.02.01.11	1.02.01.11.07	Rectifiers
1.02	1.02.01	1.02.01.11	1.02.01.11.08	Protection and Control Equipment
1.02	1.02.01	1.02.01.11	1.02.01.11.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.02	1.02.01	1.02.01.11	1.02.01.11.10	Data Connection to Control Centre
1.02	1.02.01	1.02.01.12		**Auxiliary Equipment Enclosure**
1.02	1.02.01	1.02.01.12	1.02.01.12.01	Base
1.02	1.02.01	1.02.01.12	1.02.01.12.02	Enclosure
1.02	1.02.01	1.02.01.12	1.02.01.12.03	Compound
1.02	1.02.01	1.02.01.12	1.02.01.12.04	Site Access
1.02	1.02.01	1.02.01.12	1.02.01.12.05	Switchgear Equipment
1.02	1.02.01	1.02.01.12	1.02.01.12.06	Transformers
1.02	1.02.01	1.02.01.12	1.02.01.12.07	Rectifiers
1.02	1.02.01	1.02.01.12	1.02.01.12.08	Protection and Control Equipment
1.02	1.02.01	1.02.01.12	1.02.01.12.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.02	1.02.01	1.02.01.12	1.02.01.12.10	Data Connection to Control Centre
1.02	1.02.01	1.02.01.13		**Cables and Containment**
1.02	1.02.01	1.02.01.13	1.02.01.13.01	Cable
1.02	1.02.01	1.02.01.13	1.02.01.13.02	Containment in Buildings or Structures
1.02	1.02.01	1.02.01.13	1.02.01.13.03	Tremble Devices / Theft Protection
1.02	1.02.01	1.02.01.13	1.02.01.13.04	HV Cable Terminations
1.02	1.02.01	1.02.01.14		**Testing and Commissioning**
1.02	1.02.01	1.02.01.14	1.02.01.14.01	Testing: During the Progress of the Works
1.02	1.02.01	1.02.01.14	1.02.01.14.02	Testing: On Completion of the Works
1.02	1.02.01	1.02.01.14	1.02.01.14.03	Commissioning: Work Completed in Sections
1.02	1.02.01	1.02.01.14	1.02.01.14.04	Commissioning: Co-ordination of Sectional Work
1.02	1.02.01	1.02.01.14	1.02.01.14.05	Commissioning and Handover
1.02	1.02.01	1.02.01.15		**Abandonment and Recovery of Redundant Equipment**
1.02	1.02.01	1.02.01.15	1.02.01.15.01	Switchgear Equipment
1.02	1.02.01	1.02.01.15	1.02.01.15.02	Auto Transformers (AT)
1.02	1.02.01	1.02.01.15	1.02.01.15.03	Supervisory Control and Data Acquisition (SCADA) Equipment
1.02	1.02.01	1.02.01.15	1.02.01.15.04	Cables
1.02	1.02.02			**Overhead Line Equipment (OLE)**
1.02	1.02.02	1.02.02.01		**Support Structures**
1.02	1.02.02	1.02.02.01	1.02.02.01.01	Piled Foundation
1.02	1.02.02	1.02.02.01	1.02.02.01.02	Reinforced Concrete Foundation
1.02	1.02.02	1.02.02.01	1.02.02.01.03	Single Track Cantilever

1.02	1.02.02	1.02.02.01	1.02.02.01.04	Twin Track Cantilever
1.02	1.02.02	1.02.02.01	1.02.02.01.05	Twin Cantilever
1.02	1.02.02	1.02.02.01	1.02.02.01.06	Portal
1.02	1.02.02	1.02.02.01	1.02.02.01.07	Anchor Portal
1.02	1.02.02	1.02.02.01	1.02.02.01.08	Mid-point Anchor
1.02	1.02.02	1.02.02.01	1.02.02.01.09	Headspan
1.02	1.02.02	1.02.02.01	1.02.02.01.10	Self-supporting Anchor
1.02	1.02.02	1.02.02.01	1.02.02.01.11	Back-tie
1.02	1.02.02	1.02.02.01	1.02.02.01.12	Structure Number Plate
1.02	1.02.02	1.02.02.01	1.02.02.01.13	Anti-climbing Guard
1.02	1.02.02	1.02.02.01	1.02.02.01.14	Fixings to Bridges and Viaducts
1.02	1.02.02	1.02.02.01	1.02.02.01.15	Fixings to Tunnels
1.02	1.02.02	1.02.02.02		**Small Part Steelwork (SPS)**
1.02	1.02.02	1.02.02.02	1.02.02.02.01	Support and Registration Assemblies
1.02	1.02.02	1.02.02.02	1.02.02.02.02	Earth Wire Anchor
1.02	1.02.02	1.02.02.02	1.02.02.02.03	Autotransformer 'Gibbet' Steelwork
1.02	1.02.02	1.02.02.03		**Wiring**
1.02	1.02.02	1.02.02.03	1.02.02.03.01	Contact Wire
1.02	1.02.02	1.02.02.03	1.02.02.03.02	Catenary Wire
1.02	1.02.02	1.02.02.03	1.02.02.03.03	Contenary Wire
1.02	1.02.02	1.02.02.03	1.02.02.03.04	Current Jumper
1.02	1.02.02	1.02.02.03	1.02.02.03.05	Tensioning Device
1.02	1.02.02	1.02.02.04		**Sectioning**
1.02	1.02.02	1.02.02.04	1.02.02.04.01	Isolation Devices
1.02	1.02.02	1.02.02.04	1.02.02.04.02	Insulators
1.02	1.02.02	1.02.02.04	1.02.02.04.03	Neutral Sections
1.02	1.02.02	1.02.02.05		**Depot Traction**
1.02	1.02.02	1.02.02.05	1.02.02.05.01	Overhead Tramlines
1.02	1.02.02	1.02.02.05	1.02.02.05.02	Circuit Breaker
1.02	1.02.02	1.02.02.05	1.02.02.05.03	Low Neg Shoe Detector Traction
1.02	1.02.02	1.02.02.05	1.02.02.05.04	Switches
1.02	1.02.02	1.02.02.06		**Earthing and Bonding**
1.02	1.02.02	1.02.02.06	1.02.02.06.01	Return Conductor
1.02	1.02.02	1.02.02.06	1.02.02.06.02	Earthing Conductor
1.02	1.02.02	1.02.02.06	1.02.02.06.03	Support Structure Bonds Ancillary
1.02	1.02.02	1.02.02.06	1.02.02.06.04	Structure Bonds
1.02	1.02.02	1.02.02.06	1.02.02.06.05	Return Screening Conductor
1.02	1.02.02	1.02.02.07		**Clearance to Structures**
1.02	1.02.02	1.02.02.07	1.02.02.07.01	Return Conductor
1.02	1.02.02	1.02.02.07	1.02.02.07.02	Station Canopies
1.02	1.02.02	1.02.02.07	1.02.02.07.03	Parapets
1.02	1.02.02	1.02.02.08		**Testing and Commissioning**
1.02	1.02.02	1.02.02.08	1.02.02.08.01	Testing: During the Progress of the Works
1.02	1.02.02	1.02.02.08	1.02.02.08.02	Testing: On Completion of the Works
1.02	1.02.02	1.02.02.08	1.02.02.08.03	Commissioning: Work Completed in Sections
1.02	1.02.02	1.02.02.08	1.02.02.08.04	Commissioning: Co-ordination of Sectional Work
1.02	1.02.02	1.02.02.08	1.02.02.08.04	Commissioning and Handover
1.02	1.02.02	1.02.02.09		**Abandonment and Recovery of Redundant Equipment**
1.02	1.02.02	1.02.02.09	1.02.02.09.01	Support Structures
1.02	1.02.02	1.02.02.09	1.02.02.09.02	Small Part Steelwork (SPS)
1.02	1.02.02	1.02.02.09	1.02.02.09.03	Wiring
1.02	1.02.03			**Conductor Rail**

1.02	1.02.03	1.02.03.01		**Contact Rail System**
1.02	1.02.03	1.02.03.01	1.02.03.01.01	Conductor Rail
1.02	1.02.03	1.02.03.01	1.02.03.01.02	Return Conductor Rail
1.02	1.02.03	1.02.03.01	1.02.03.01.03	Ramps
1.02	1.02.03	1.02.03.01	1.02.03.01.04	Track Isolating Switch: state type
1.02	1.02.03	1.02.03.01	1.02.03.01.05	Guard Boards
1.02	1.02.03	1.02.03.02		**Earthing and Bonding**
1.02	1.02.03	1.02.03.02	1.02.03.02.01	Flashover Strips
1.02	1.02.03	1.02.03.02	1.02.03.02.02	Rail to Rail Bonds
1.02	1.02.03	1.02.03.02	1.02.03.02.03	Electric Traction Equipment (ETE)
1.02	1.02.03	1.02.03.02	1.02.03.02.04	Structure to Rail Bonds
1.02	1.02.03	1.02.03.02	1.02.03.02.05	Spider Plate Bonds
1.02	1.02.03	1.02.03.03		**Testing and Commissioning**
1.02	1.02.03	1.02.03.03	1.02.03.03.01	Testing: During the Progress of the Works
1.02	1.02.03	1.02.03.03	1.02.03.03.02	Testing: On Completion of the Works
1.02	1.02.03	1.02.03.03	1.02.03.03.03	Commissioning: Work Completed in Sections
1.02	1.02.03	1.02.03.03	1.02.03.03.04	Commissioning: Co-ordination of Sectional Work
1.02	1.02.03	1.02.03.03	1.02.03.03.05	Commissioning and Handover
1.02	1.02.03	1.02.03.04		**Abandonment and Recovery of Redundant Equipment**
1.02	1.02.03	1.02.03.04	1.02.03.04.01	Contact Rail System: state details
1.02	1.02.03	1.02.03.04	1.02.03.04.02	Earthing and Bonding : state details

Level 1	Level 2	Level 3	Level 4	Item
1.03				**Electric Power and Plant**
1.03	1.03.01			**Primary Power Supply**
1.03	1.03.01	1.03.01.01		**Main Grid Substation**
1.03	1.03.01	1.03.01.01	1.03.01.01.01	Base
1.03	1.03.01	1.03.01.01	1.03.01.01.02	Enclosure
1.03	1.03.01	1.03.01.01	1.03.01.01.03	Compound
1.03	1.03.01	1.03.01.01	1.03.01.01.04	Site Access
1.03	1.03.01	1.03.01.01	1.03.01.01.05	Substation Equipment
1.03	1.03.01	1.03.01.01	1.03.01.01.06	Transformers
1.03	1.03.01	1.03.01.01	1.03.01.01.07	Rectifiers
1.03	1.03.01	1.03.01.01	1.03.01.01.08	Protection and Control Equipment
1.03	1.03.01	1.03.01.01	1.03.01.01.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.03	1.03.01	1.03.01.01	1.03.01.01.10	Data Connection to Control Centre
1.03	1.03.01	1.03.01.02		**Distribution Network Operator (DNO) Substation**
1.03	1.03.01	1.03.01.02	1.03.01.02.01	Base
1.03	1.03.01	1.03.01.02	1.03.01.02.02	Enclosure
1.03	1.03.01	1.03.01.02	1.03.01.02.03	Compound
1.03	1.03.01	1.03.01.02	1.03.01.02.04	Site Access
1.03	1.03.01	1.03.01.02	1.03.01.02.05	Substation Equipment
1.03	1.03.01	1.03.01.02	1.03.01.02.06	Transformers
1.03	1.03.01	1.03.01.02	1.03.01.02.07	Rectifiers
1.03	1.03.01	1.03.01.02	1.03.01.02.08	Protection and Control Equipment
1.03	1.03.01	1.03.01.02	1.03.01.02.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.03	1.03.01	1.03.01.02	1.03.01.02.10	Data Connection to Control Centre
1.03	1.03.01	1.03.01.03		**Private Electricity Generation**
1.03	1.03.01	1.03.01.03	1.03.01.03.01	Base
1.03	1.03.01	1.03.01.03	1.03.01.03.02	Enclosure
1.03	1.03.01	1.03.01.03	1.03.01.03.03	Compound
1.03	1.03.01	1.03.01.03	1.03.01.03.04	Site Access
1.03	1.03.01	1.03.01.03	1.03.01.03.05	Substation Equipment
1.03	1.03.01	1.03.01.03	1.03.01.03.06	Transformers
1.03	1.03.01	1.03.01.03	1.03.01.03.07	Rectifiers
1.03	1.03.01	1.03.01.03	1.03.01.03.08	Protection and Control Equipment
1.03	1.03.01	1.03.01.03	1.03.01.03.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.03	1.03.01	1.03.01.03	1.03.01.03.10	Data Connection to Control Centre
1.03	1.03.01	1.03.01.04		**Power Transformation Device**
1.03	1.03.01	1.03.01.04	1.03.01.04.01	Base
1.03	1.03.01	1.03.01.04	1.03.01.04.02	Enclosure
1.03	1.03.01	1.03.01.04	1.03.01.04.03	Compound
1.03	1.03.01	1.03.01.04	1.03.01.04.04	Site Access
1.03	1.03.01	1.03.01.04	1.03.01.04.05	Substation Equipment
1.03	1.03.01	1.03.01.04	1.03.01.04.06	Transformers
1.03	1.03.01	1.03.01.04	1.03.01.04.07	Rectifiers
1.03	1.03.01	1.03.01.04	1.03.01.04.08	Protection and Control Equipment
1.03	1.03.01	1.03.01.04	1.03.01.04.09	Supervisory Control and Data Acquisition (SCADA) Equipment
1.03	1.03.01	1.03.01.04	1.03.01.04.10	Data Connection to Control Centre
1.03	1.03.01	1.03.01.05		**Small Power for Equipment**
1.03	1.03.01	1.03.01.05	1.03.01.05.01	DNO Power Cubicle
1.03	1.03.01	1.03.01.05	1.03.01.05.02	Principal Supply Point (PSP)
1.03	1.03.01	1.03.01.05	1.03.01.05.03	Auxiliary Supply Points (ASP)
1.03	1.03.01	1.03.01.05	1.03.01.05.04	Functional Supply Points (FSP)

1.03	1.03.01	1.03.01.05	1.03.01.05.05	Feeder Protection Panel
1.03	1.03.01	1.03.01.06		**Earthing and Bonding**
1.03	1.03.01	1.03.01.06	1.03.01.06.01	Isolation Devices
1.03	1.03.01	1.03.01.06	1.03.01.06.02	Insulators
1.03	1.03.01	1.03.01.06	1.03.01.06.03	Earthing
1.03	1.03.01	1.03.01.06	1.03.01.06.04	Lightning Protection
1.03	1.03.01	1.03.01.06	1.03.01.06.05	Main Protective Bonding Conductor
1.03	1.03.01	1.03.01.06	1.03.01.06.06	Supplementary Bonding Conductors
1.03	1.03.01	1.03.01.07		**Cables and Containment**
1.03	1.03.01	1.03.01.07	1.03.01.07.01	Cable
1.03	1.03.01	1.03.01.07	1.03.01.07.02	Containment in Buildings or Structures
1.03	1.03.01	1.03.01.08		**Testing and Commissioning**
1.03	1.03.01	1.03.01.08	1.03.01.08.01	Testing: During the Progress of the works
1.03	1.03.01	1.03.01.08	1.03.01.08.02	Testing: On completion of the works
1.03	1.03.01	1.03.01.08	1.03.01.08.03	Commissioning: Work completed in sections
1.03	1.03.01	1.03.01.08	1.03.01.08.04	Commissioning: Co-ordination of Sectional Work
1.03	1.03.01	1.03.01.08	1.03.01.08.05	Commissioning and Handover
1.03	1.03.01	1.03.01.09		**Abandonment and Recovery of Redundant Equipment**
1.03	1.03.01	1.03.01.09	1.03.01.09.01	Sub-station Equipment
1.03	1.03.01	1.03.01.09	1.03.01.09.02	Transformer
1.03	1.03.01	1.03.01.09	1.03.01.09.03	Rectifier
1.03	1.03.01	1.03.01.09	1.03.01.09.04	Protection and Control Equipment
1.03	1.03.01	1.03.01.09	1.03.01.09.05	Supervisory Control and Data Acquisition (SCADA) Equipment
1.03	1.03.01	1.03.01.09	1.03.01.09.06	Cables
1.03	1.03.02			**Plant and Equipment**
1.03	1.03.02	1.03.02.01		**Plant and Equipment: Lineside**
1.03	1.03.02	1.03.02.01	1.03.02.01.01	Rail Heaters
1.03	1.03.02	1.03.02.01	1.03.02.01.02	Points Heaters
1.03	1.03.02	1.03.02.01	1.03.02.01.03	Junction Lighting
1.03	1.03.02	1.03.02.02		**Plant and Equipment- Maintenance**
1.03	1.03.02	1.03.02.02	1.03.02.02.01	General Equipment
1.03	1.03.02	1.03.02.02	1.03.02.02.02	Workshop Equipment
1.03	1.03.02	1.03.02.02	1.03.02.02.03	Cleaning Equipment
1.03	1.03.02	1.03.02.02	1.03.02.02.04	Lifting Equipment
1.03	1.03.02	1.03.02.02	1.03.02.02.05	De-icing Equipment
1.03	1.03.02	1.03.02.02	1.03.02.02.06	Overhead Trolley
1.03	1.03.02	1.03.02.02	1.03.02.02.07	Access Equipment
1.03	1.03.02	1.03.02.02	1.03.02.02.08	Battery Equipment
1.03	1.03.02	1.03.02.02	1.03.02.02.09	Compressed Air Equipment
1.03	1.03.02	1.03.02.02	1.03.02.02.10	Calibration
1.03	1.03.02	1.03.02.02	1.03.02.02.11	Gauge Equipment
1.03	1.03.02	1.03.02.02	1.03.02.02.12	Train Test Equipment
1.03	1.03.02	1.03.02.02	1.03.02.02.13	Train Monitoring Equipment
1.03	1.03.02	1.03.02.02	1.03.02.02.14	Welding Equipment
1.03	1.03.02	1.03.02.02	1.03.02.02.15	Safety Equipment
1.03	1.03.02	1.03.02.02	1.03.02.02.16	Wheel Lathe
1.03	1.03.02	1.03.02.02	1.03.02.02.17	Electrical Portable Appliances
1.03	1.03.02	1.03.02.03		**Plant and Equipment - Operational**
1.03	1.03.02	1.03.02.03	1.03.02.03.01	Chemical Effluent Toilet (CET) Point
1.03	1.03.02	1.03.02.03	1.03.02.03.02	Carriage Washing Plant
1.03	1.03.02	1.03.02.03	1.03.02.03.03	Carriage Watering System
1.03	1.03.02	1.03.02.03	1.03.02.03.04	Sanding System Point

1.03	1.03.02	1.03.02.03	1.03.02.03.05	Diesel Fuelling Point
1.03	1.03.02	1.03.02.04		**Testing and Commissioning**
1.03	1.03.02	1.03.02.04	1.03.02.04.01	Testing: During the Progress of the Works
1.03	1.03.02	1.03.02.04	1.03.02.04.02	Testing: On Completion of the Works
1.03	1.03.02	1.03.02.04	1.03.02.04.03	Commissioning: Work Completed in Sections
1.03	1.03.02	1.03.02.04	1.03.02.04.04	Commissioning: Co-ordination of Sectional Work
1.03	1.03.02	1.03.02.04	1.03.02.04.05	Commissioning and Handover
1.03	1.03.02	1.03.02.05		**Abandonment and Recovery of Redundant Equipment**
1.03	1.03.02	1.03.02.05	1.03.02.05.01	Lineside Equipment
1.03	1.03.02	1.03.02.05	1.03.02.05.02	Maintenance Equipment
1.03	1.03.02	1.03.02.05	1.03.02.05.03	Operational Equipment
1.03	1.03.02	1.03.02.05	1.03.02.05.04	Depot Traction

Level 1	Level 2	Level 3	Level 4	Item
1.04				**Permanent Way**
1.04	1.04.01			**Plain Line**
1.04	1.04.01	1.04.01.01		**Ballast Track**
1.04	1.04.01	1.04.01.01	1.04.01.01.01	Track Ballast: state width and depth
1.04	1.04.01	1.04.01.01	1.04.01.01.02	Sleepers: state type, fixings and spacing
1.04	1.04.01	1.04.01.01	1.04.01.01.03	Running Rails: state profile, jointing type and curvature
1.04	1.04.01	1.04.01.02		**Slab Track**
1.04	1.04.01	1.04.01.02	1.04.01.02.01	Track Slab: state section and reinforcement details
1.04	1.04.01	1.04.01.02	1.04.01.02.02	Sleepers: state type, fixings and spacing
1.04	1.04.01	1.04.01.02	1.04.01.02.03	Running Rails: state profile, jointing type and curvature
1.04	1.04.01	1.04.01.03		**Longitudinal Bearer Track**
1.04	1.04.01	1.04.01.03	1.04.01.03.01	Longitudinal Bearers: state type, fixings and section
1.04	1.04.01	1.04.01.03	1.04.01.03.02	Sleepers: state type, fixings and spacing
1.04	1.04.01	1.04.01.03	1.04.01.03.03	Running Rails: state profile, jointing type and curvature
1.04	1.04.01	1.04.01.04		**Ancillaries**
1.04	1.04.01	1.04.01.04	1.04.01.04.01	Check Rails: state type
1.04	1.04.01	1.04.01.04	1.04.01.04.02	Guard Rails: state type
1.04	1.04.01	1.04.01.04	1.04.01.04.03	Rail Lubricators: state type
1.04	1.04.01	1.04.01.04	1.04.01.04.04	Cable Management Sleepers
1.04	1.04.01	1.04.01.04	1.04.01.04.05	Buffer Stops
1.04	1.04.01	1.04.01.04	1.04.01.04.06	Other Ancillaries
1.04	1.04.02			**Switches and Crossing**
1.04	1.04.02	1.04.02.01		**Ballast Track**
1.04	1.04.02	1.04.02.01	1.04.02.01.01	Trap
1.04	1.04.02	1.04.02.01	1.04.02.01.02	Turnout
1.04	1.04.02	1.04.02.01	1.04.02.01.03	Crossover
1.04	1.04.02	1.04.02.01	1.04.02.01.04	Diamond: state type
1.04	1.04.02	1.04.02.01	1.04.02.01.05	Scissor Crossover
1.04	1.04.02	1.04.02.01	1.04.02.01.06	Double Junction: Diamond: state type
1.04	1.04.02	1.04.02.01	1.04.02.01.07	Three Line Crossover: Diamond: state type
1.04	1.04.02	1.04.02.01	1.04.02.01.08	Tandem Turnout
1.04	1.04.02	1.04.02.01	1.04.02.01.09	Other: state type, size and details
1.04	1.04.02	1.04.02.02		**Slab Track**
1.04	1.04.02	1.04.02.02	1.04.02.02.01	Trap
1.04	1.04.02	1.04.02.02	1.04.02.02.02	Turnout
1.04	1.04.02	1.04.02.02	1.04.02.02.03	Crossover
1.04	1.04.02	1.04.02.02	1.04.02.02.04	Diamond: state type
1.04	1.04.02	1.04.02.02	1.04.02.02.05	Scissor Crossover
1.04	1.04.02	1.04.02.02	1.04.02.02.06	Double Junction: Diamond: state type
1.04	1.04.02	1.04.02.02	1.04.02.02.07	Three Line Crossover: Diamond: state type
1.04	1.04.02	1.04.02.02	1.04.02.02.08	Tandem Turnout
1.04	1.04.02	1.04.02.02	1.04.02.02.09	Other: state type, size and details
1.04	1.04.02	1.04.02.03		**Longitudinal Bearer Track**
1.04	1.04.02	1.04.02.03	1.04.02.03.01	Trap
1.04	1.04.02	1.04.02.03	1.04.02.03.02	Turnout
1.04	1.04.02	1.04.02.03	1.04.02.03.03	Crossover
1.04	1.04.02	1.04.02.03	1.04.02.03.04	Diamond: state type
1.04	1.04.02	1.04.02.03	1.04.02.03.05	Scissor Crossover
1.04	1.04.02	1.04.02.03	1.04.02.03.06	Double Junction: Diamond: state type
1.04	1.04.02	1.04.02.03	1.04.02.03.07	Three Line Crossover: Diamond: state type
1.04	1.04.02	1.04.02.03	1.04.02.03.08	Tandem Turnout
1.04	1.04.02	1.04.02.03	1.04.02.03.09	Other: state type, size and details
1.04	1.04.02	1.04.02.04		**Ancillaries**

1.04	1.04.02	1.04.02.04	1.04.02.04.01	Cable Management Sleepers
1.04	1.04.02	1.04.02.04	1.04.02.04.02	Lateral Resistance Plates
1.04	1.04.02	1.04.02.04	1.04.02.04.03	Sand Drag: state dimensions
1.04	1.04.02	1.04.02.04	1.04.02.04.04	Other Ancillaries: state type
1.04	1.04.03			**Lifting, Packing, Slewing and Lowering of Existing Track**
1.04	1.04.03	1.04.03.01		**Plain Line**
1.04	1.04.03	1.04.03.01	1.04.03.01.01	Ballast Track
1.04	1.04.03	1.04.03.01	1.04.03.01.02	Longitudinal Bearer Track
1.04	1.04.03	1.04.03.01	1.04.03.01.03	Ancillaries: state type
1.04	1.04.03	1.04.03.02		**Switches and Crossing**
1.04	1.04.03	1.04.03.02	1.04.03.02.01	Switches and Crossing: state layout
1.04	1.04.03	1.04.03.02	1.04.03.02.02	Ancillaries: state type
1.04	1.04.04			**Abandonment, Recovery and Disposal of Redundant Equipment**
1.04	1.04.04	1.04.04.01		**Plain Line**
1.04	1.04.04	1.04.04.01	1.04.04.01.01	Ballast Track
1.04	1.04.04	1.04.04.01	1.04.04.01.02	Slab Track
1.04	1.04.04	1.04.04.01	1.04.04.01.03	Longitudinal Bearer Track
1.04	1.04.04	1.04.04.01	1.04.04.01.04	Ancillaries
1.04	1.04.04	1.04.04.02		**Switches and Crossing**
1.04	1.04.04	1.04.04.02	1.04.04.02.01	Switches and Crossing: state size and layout
1.04	1.04.04	1.04.04.02	1.04.04.02.02	Ancillaries

Level 1	Level 2	Level 3	Level 4	Item
1.05				**Operational Telecommunications Systems**
1.05	1.05.01			**Control Centre**
1.05	1.05.01	1.05.01.01		**Visual Display Unit (VDU)**
1.05	1.05.01	1.05.01.01	1.05.01.01.01	State type and model reference
1.05	1.05.01	1.05.01.02		**Entrance – Exit System (Signal Box Control Panel)**
1.05	1.05.01	1.05.01.02	1.05.01.02.01	State type and model reference
1.05	1.05.02			**Operational Radio**
1.05	1.05.02	1.05.02.01		**Radio Equipment**
1.05	1.05.02	1.05.02.01	1.05.02.01.01	Masts
1.05	1.05.02	1.05.02.01	1.05.02.01.02	Aerials
1.05	1.05.02	1.05.02.01	1.05.02.01.03	Base Stations
1.05	1.05.03			**Data Transmission**
1.05	1.05.03	1.05.03.01		**Transmission Network**
1.05	1.05.03	1.05.03.01	1.05.03.01.01	State type
1.05	1.05.03	1.05.03.02		**Transmission Equipment**
1.05	1.05.03	1.05.03.02	1.05.03.02.01	PCM: Digital
1.05	1.05.03	1.05.03.02	1.05.03.02.02	Drop and Insert: Digital Circuit
1.05	1.05.03	1.05.03.02	1.05.03.02.03	Carrier: Analogue
1.05	1.05.04			**Cables**
1.05	1.05.04	1.05.04.01		**Copper**
1.05	1.05.04	1.05.04.01	1.05.04.01.01	Conductor
1.05	1.05.04	1.05.04.02		**Fibre Optic**
1.05	1.05.04	1.05.04.02	1.05.04.02.01	Conductor
1.05	1.05.04	1.05.04.03		**Composite**
1.05	1.05.04	1.05.04.03	1.05.04.03.01	Conductor
1.05	1.05.04	1.05.04.04		**Other Stated Material**
1.05	1.05.04	1.05.04.04	1.05.04.04.01	Conductor
1.05	1.05.05			**Concentrator Equipment**
1.05	1.05.05	1.05.05.01		**Telephone Concentrators**
1.05	1.05.05	1.05.05.01	1.05.05.01.01	Large > 64 Lines
1.05	1.05.05	1.05.05.01	1.05.05.01.02	Medium 32 to 64 Lines
1.05	1.05.05	1.05.05.01	1.05.05.01.03	Small < 32 Lines
1.05	1.05.05	1.05.05.02		**Other Stated Concentrators**
1.05	1.05.05	1.05.05.02	1.05.05.02.01	Large > 64 Lines
1.05	1.05.05	1.05.05.02	1.05.05.02.02	Medium 32 to 64 Lines
1.05	1.05.05	1.05.05.02	1.05.05.02.03	Small < 32 Lines
1.05	1.05.05	1.05.05.03		**Operational Radio**
1.05	1.05.05	1.05.05.03	1.05.05.03.01	Large > 64 Lines
1.05	1.05.05	1.05.05.03	1.05.05.03.02	Medium 32 to 64 Lines
1.05	1.05.05	1.05.05.03	1.05.05.03.03	Small < 32 Lines
1.05	1.05.05	1.05.05.04		**Zone Control Communication**
1.05	1.05.05	1.05.05.04	1.05.05.04.01	Large > 64 Lines
1.05	1.05.05	1.05.05.04	1.05.05.04.02	Medium 32 to 64 Lines
1.05	1.05.05	1.05.05.04	1.05.05.04.03	Small < 32 Lines
1.05	1.05.06			**Operational Telephones**
1.05	1.05.06	1.05.06.01		**Access Point**
1.05	1.05.06	1.05.06.01	1.05.06.01.01	State type and model reference
1.05	1.05.06	1.05.06.02		**Direct Line**
1.05	1.05.06	1.05.06.02	1.05.06.02.01	State type and model reference
1.05	1.05.06	1.05.06.03		**Emergency**
1.05	1.05.06	1.05.06.03	1.05.06.03.01	State type and model reference
1.05	1.05.06	1.05.06.04		**Line Side Plug**
1.05	1.05.06	1.05.06.04	1.05.06.04.01	State type and model reference
1.05	1.05.06	1.05.06.05		**Emergency Telephone Devices (ETD)**
1.05	1.05.06	1.05.06.05	1.05.06.05.01	State type and model reference

1.05	1.05.06	1.05.06.06		**Signal Post Telephone (SPT)**
1.05	1.05.06	1.05.06.06	1.05.06.06.01	State type and model reference
1.05	1.05.06	1.05.06.07		**Point Zone Telephone (PZT)**
1.05	1.05.06	1.05.06.07	1.05.06.07.01	State type and model reference
1.05	1.05.06	1.05.06.08		**Ground Frame Circuit**
1.05	1.05.06	1.05.06.08	1.05.06.08.01	State type and model reference
1.05	1.05.06	1.05.06.09		**Tunnel Emergency Circuit**
1.05	1.05.06	1.05.06.09	1.05.06.09.01	State type and model reference
1.05	1.05.06	1.05.06.10		**Level Crossing: Public Emergency Telephone System (PETS)**
1.05	1.05.06	1.05.06.10	1.05.06.10.01	State type and model reference
1.05	1.05.07			**Audio-visual Management Systems**
1.05	1.05.07	1.05.07.01		**Driver-only Operating Systems**
1.05	1.05.07	1.05.07.01	1.05.07.01.01	CCTV Cameras
1.05	1.05.07	1.05.07.01	1.05.07.01.02	Monitors
1.05	1.05.07	1.05.07.01	1.05.07.01.03	Mirrors
1.05	1.05.07	1.05.07.01	1.05.07.01.04	Control Panels
1.05	1.05.07	1.05.07.01	1.05.07.01.05	Microphones and Speaking Points
1.05	1.05.07	1.05.07.01	1.05.07.01.06	Recorders
1.05	1.05.07	1.05.07.01	1.05.07.01.07	Amplifiers
1.05	1.05.07	1.05.07.01	1.05.07.01.08	Primary Object Detectors (POD)
1.05	1.05.07	1.05.07.01	1.05.07.01.09	Complementary Object Detectors (COD)
1.05	1.05.07	1.05.07.02		**Timetable Management Systems**
1.05	1.05.07	1.05.07.02	1.05.07.02.01	CCTV Cameras
1.05	1.05.07	1.05.07.02	1.05.07.02.02	Monitors
1.05	1.05.07	1.05.07.02	1.05.07.02.03	Mirrors
1.05	1.05.07	1.05.07.02	1.05.07.02.04	Control Panels
1.05	1.05.07	1.05.07.02	1.05.07.02.05	Microphones and Speaking Points
1.05	1.05.07	1.05.07.02	1.05.07.02.06	Recorders
1.05	1.05.07	1.05.07.02	1.05.07.02.07	Amplifiers
1.05	1.05.07	1.05.07.02	1.05.07.02.08	Primary Object Detectors (POD)
1.05	1.05.07	1.05.07.02	1.05.07.02.09	Complementary Object Detectors (COD)
1.05	1.05.07	1.05.07.03		**Security Systems**
1.05	1.05.07	1.05.07.03	1.05.07.03.01	CCTV Cameras
1.05	1.05.07	1.05.07.03	1.05.07.03.02	Monitors
1.05	1.05.07	1.05.07.03	1.05.07.03.03	Mirrors
1.05	1.05.07	1.05.07.03	1.05.07.03.04	Control Panels
1.05	1.05.07	1.05.07.03	1.05.07.03.05	Microphones and Speaking Points
1.05	1.05.07	1.05.07.03	1.05.07.03.06	Recorders
1.05	1.05.07	1.05.07.03	1.05.07.03.07	Amplifiers
1.05	1.05.07	1.05.07.03	1.05.07.03.08	Primary Object Detectors (POD)
1.05	1.05.07	1.05.07.03	1.05.07.03.09	Complementary Object Detectors (COD)
1.05	1.05.07	1.05.07.04		**Surveillance Systems**
1.05	1.05.07	1.05.07.04	1.05.07.04.01	CCTV Cameras
1.05	1.05.07	1.05.07.04	1.05.07.04.02	Monitors
1.05	1.05.07	1.05.07.04	1.05.07.04.03	Mirrors
1.05	1.05.07	1.05.07.04	1.05.07.04.04	Control Panels
1.05	1.05.07	1.05.07.04	1.05.07.04.05	Microphones and Speaking Points
1.05	1.05.07	1.05.07.04	1.05.07.04.06	Recorders
1.05	1.05.07	1.05.07.04	1.05.07.04.07	Amplifiers
1.05	1.05.07	1.05.07.04	1.05.07.04.08	Primary Object Detectors (POD)
1.05	1.05.07	1.05.07.04	1.05.07.04.09	Complementary Object Detectors (COD)
1.05	1.05.08			**Positioning Equipment**
1.05	1.05.08	1.05.08.01		**Train Positioning Systems**
1.05	1.05.08	1.05.08.01	1.05.08.01.01	Automatic Train Reporting (ATR)
1.05	1.05.08	1.05.08.01	1.05.08.01.02	Station Information VDU Stepping (SIVS)
1.05	1.05.08	1.05.08.01	1.05.08.01.03	Train Running Under System TOPS (TRUST)
1.05	1.05.09			**Remote Asset Monitoring Systems**

1.05	1.05.09	1.05.09.01		**Assets: Track**
1.05	1.05.09	1.05.09.01	1.05.09.01.01	Point Heaters
1.05	1.05.09	1.05.09.01	1.05.09.01.02	Standby Generators
1.05	1.05.09	1.05.09.01	1.05.09.01.03	Pumps
1.05	1.05.09	1.05.09.01	1.05.09.01.04	SCADA Installation
1.05	1.05.09	1.05.09.01	1.05.09.01.05	Relocatable Equipment Buildings (REB)
1.05	1.05.09	1.05.09.02		**Assets: Plant**
1.05	1.05.09	1.05.09.02	1.05.09.02.01	Point Heaters
1.05	1.05.09	1.05.09.02	1.05.09.02.02	Standby Generators
1.05	1.05.09	1.05.09.02	1.05.09.02.03	Pumps
1.05	1.05.09	1.05.09.02	1.05.09.02.04	SCADA Installation
1.05	1.05.09	1.05.09.02	1.05.09.02.05	Relocatable Equipment Buildings (REB)
1.05	1.05.10			**Customer Information System (CIS)**
1.05	1.05.10	1.05.10.01		**Audio**
1.05	1.05.10	1.05.10.01	1.05.10.01.01	Speakers
1.05	1.05.10	1.05.10.01	1.05.10.01.02	Microphones and Speaking Points
1.05	1.05.10	1.05.10.01	1.05.10.01.03	Amplifier
1.05	1.05.10	1.05.10.01	1.05.10.01.04	Ambient Noise Sensor
1.05	1.05.10	1.05.10.01	1.05.10.01.05	Control Panels
1.05	1.05.10	1.05.10.02		**Video**
1.05	1.05.10	1.05.10.02	1.05.10.02.01	Video Display Units
1.05	1.05.10	1.05.10.02	1.05.10.02.02	Recorders
1.05	1.05.10	1.05.10.02	1.05.10.02.03	Control Panels
1.05	1.05.10	1.05.10.03		**Clocks**
1.05	1.05.10	1.05.10.03	1.05.10.03.01	Analogue
1.05	1.05.10	1.05.10.03	1.05.10.03.02	Digital
1.05	1.05.11			**Equipment Housings, Platforms and Foundations**
1.05	1.05.11	1.05.11.01		**Location Case: complete with Racking and Equipment: state type**
1.05	1.05.11	1.05.11.01	1.05.11.01.01	Housing
1.05	1.05.11	1.05.11.01	1.05.11.01.02	Racking
1.05	1.05.11	1.05.11.01	1.05.11.01.03	Services
1.05	1.05.11	1.05.11.01	1.05.11.01.04	Foundation
1.05	1.05.11	1.05.11.02		**Portable Relocatable Equipment Building (REB): complete with Servi**
1.05	1.05.11	1.05.11.02	1.05.11.02.01	Housing
1.05	1.05.11	1.05.11.02	1.05.11.02.02	Racking
1.05	1.05.11	1.05.11.02	1.05.11.02.03	Services
1.05	1.05.11	1.05.11.02	1.05.11.02.04	Foundation
1.05	1.05.11	1.05.11.03		**Trackside Equipment: Level Ground: state type and foundation**
1.05	1.05.11	1.05.11.03	1.05.11.03.01	Housing
1.05	1.05.11	1.05.11.03	1.05.11.03.02	Racking
1.05	1.05.11	1.05.11.03	1.05.11.03.03	Services
1.05	1.05.11	1.05.11.03	1.05.11.03.04	Foundation
1.05	1.05.11	1.05.11.04		**Trackside Equipment: Staging: state type and foundation**
1.05	1.05.11	1.05.11.04	1.05.11.04.01	Housing
1.05	1.05.11	1.05.11.04	1.05.11.04.02	Racking
1.05	1.05.11	1.05.11.04	1.05.11.04.03	Services
1.05	1.05.11	1.05.11.04	1.05.11.04.04	Foundation
1.05	1.05.12			**Testing & Commissioning**
1.05	1.05.12	1.05.12.01		**Workstation**
1.05	1.05.12	1.05.12.01	1.05.12.01.01	Phased: state timing
1.05	1.05.12	1.05.12.01	1.05.12.01.02	On Completion
1.05	1.05.12	1.05.12.02		**Technical Verification**
1.05	1.05.12	1.05.12.02	1.05.12.02.01	Phased: state timing
1.05	1.05.12	1.05.12.02	1.05.12.02.02	On Completion
1.05	1.05.12	1.05.12.03		**Functional (including Through Testing)**
1.05	1.05.12	1.05.12.03	1.05.12.03.01	Phased: state timing
1.05	1.05.12	1.05.12.03	1.05.12.03.02	On Completion

1.05	1.05.12	1.05.12.04		**Commissioning and Handover**
1.05	1.05.12	1.05.12.04	1.05.12.04.01	Phased: state timing
1.05	1.05.12	1.05.12.04	1.05.12.04.02	On Completion
1.05	1.05.12	1.05.12.05		**Training of Staff**
1.05	1.05.12	1.05.12.05	1.05.12.05.01	Phased: state timing
1.05	1.05.12	1.05.12.05	1.05.12.05.02	On Completion
1.05	1.05.13			**Strategic Spares**
1.05	1.05.13	1.05.13.01		**Spares**
1.05	1.05.13	1.05.13.01	1.05.13.01.01	State system spares required
1.05	1.05.14			**Abandonment, Recovery and Disposal of Redundant Equipment**
1.05	1.05.14	1.05.14.01		**Control Centre**
1.05	1.05.14	1.05.14.01	1.05.14.01.01	Abandonment
1.05	1.05.14	1.05.14.01	1.05.14.01.02	Recovery
1.05	1.05.14	1.05.14.01	1.05.14.01.03	Disposal of Redundant Equipment
1.05	1.05.14	1.05.14.02		**Operational Radio**
1.05	1.05.14	1.05.14.02	1.05.14.02.01	Abandonment
1.05	1.05.14	1.05.14.02	1.05.14.02.02	Recovery
1.05	1.05.14	1.05.14.02	1.05.14.02.03	Disposal of Redundant Equipment
1.05	1.05.14	1.05.14.03		**Data Transmission**
1.05	1.05.14	1.05.14.03	1.05.14.03.01	Abandonment
1.05	1.05.14	1.05.14.03	1.05.14.03.02	Recovery
1.05	1.05.14	1.05.14.03	1.05.14.03.03	Disposal of Redundant Equipment
1.05	1.05.14	1.05.14.04		**Cables**
1.05	1.05.14	1.05.14.04	1.05.14.04.01	Abandonment
1.05	1.05.14	1.05.14.04	1.05.14.04.02	Recovery
1.05	1.05.14	1.05.14.04	1.05.14.04.03	Disposal of Redundant Equipment
1.05	1.05.14	1.05.14.05		**Concentrator Equipment**
1.05	1.05.14	1.05.14.05	1.05.14.05.01	Abandonment
1.05	1.05.14	1.05.14.05	1.05.14.05.02	Recovery
1.05	1.05.14	1.05.14.05	1.05.14.05.03	Disposal of Redundant Equipment
1.05	1.05.14	1.05.14.06		**Operational Telephones**
1.05	1.05.14	1.05.14.06	1.05.14.06.01	Abandonment
1.05	1.05.14	1.05.14.06	1.05.14.06.02	Recovery
1.05	1.05.14	1.05.14.06	1.05.14.06.03	Disposal of Redundant Equipment
1.05	1.05.14	1.05.14.07		**Audio-visual Management Systems**
1.05	1.05.14	1.05.14.07	1.05.14.07.01	Abandonment
1.05	1.05.14	1.05.14.07	1.05.14.07.02	Recovery
1.05	1.05.14	1.05.14.07	1.05.14.07.03	Disposal of Redundant Equipment
1.05	1.05.14	1.05.14.08		**Positioning Equipment**
1.05	1.05.14	1.05.14.08	1.05.14.08.01	Abandonment
1.05	1.05.14	1.05.14.08	1.05.14.08.02	Recovery
1.05	1.05.14	1.05.14.08	1.05.14.08.03	Disposal of Redundant Equipment
1.05	1.05.14	1.05.14.09		**Remote Asset Monitoring Systems**
1.05	1.05.14	1.05.14.09	1.05.14.09.01	Abandonment
1.05	1.05.14	1.05.14.09	1.05.14.09.02	Recovery
1.05	1.05.14	1.05.14.09	1.05.14.09.03	Disposal of Redundant Equipment
1.05	1.05.14	1.05.14.10		**Customer Information Systems**
1.05	1.05.14	1.05.14.10	1.05.14.10.01	Abandonment
1.05	1.05.14	1.05.14.10	1.05.14.10.02	Recovery
1.05	1.05.14	1.05.14.10	1.05.14.10.03	Disposal of Redundant Equipment
1.05	1.05.14	1.05.14.11		**Equipment Housings, Platforms and Foundations**
1.05	1.05.14	1.05.14.11	1.05.14.11.01	Abandonment
1.05	1.05.14	1.05.14.11	1.05.14.11.02	Recovery
1.05	1.05.14	1.05.14.11	1.05.14.11.03	Disposal of Redundant Equipment

Level 1	Level 2	Level 3	Level 4	Item
1.06				**Buildings & Property**
1.06	1.06.01			**Substructure**
1.06	1.06.01	1.06.01.01		**Substructure**
1.06	1.06.01	1.06.01.01	1.06.01.01.01	Standard Foundations
1.06	1.06.01	1.06.01.01	1.06.01.01.02	Specialist Foundations
1.06	1.06.01	1.06.01.01	1.06.01.01.03	Lowest Floor Construction
1.06	1.06.01	1.06.01.01	1.06.01.01.04	Basement Excavation
1.06	1.06.01	1.06.01.01	1.06.01.01.05	Basement Retaining Walls
1.06	1.06.02			**Superstructure**
1.06	1.06.02	1.06.02.01		**Frame**
1.06	1.06.02	1.06.02.01	1.06.02.01.01	Steel Frames
1.06	1.06.02	1.06.02.01	1.06.02.01.02	Space Frames / Decks
1.06	1.06.02	1.06.02.01	1.06.02.01.03	Concrete Casings to Steel Frames
1.06	1.06.02	1.06.02.01	1.06.02.01.04	Concrete Frames
1.06	1.06.02	1.06.02.01	1.06.02.01.05	Timber Frames
1.06	1.06.02	1.06.02.01	1.06.02.01.06	Specialist Frames
1.06	1.06.02	1.06.02.02		**Upper Floors**
1.06	1.06.02	1.06.02.02	1.06.02.02.01	Floors
1.06	1.06.02	1.06.02.02	1.06.02.02.02	Balconies
1.06	1.06.02	1.06.02.02	1.06.02.02.03	Drainage to Balconies
1.06	1.06.02	1.06.02.03		**Roof**
1.06	1.06.02	1.06.02.03	1.06.02.03.01	Roof Structure
1.06	1.06.02	1.06.02.03	1.06.02.03.02	Roof Coverings
1.06	1.06.02	1.06.02.03	1.06.02.03.03	Specialist Roof Systems
1.06	1.06.02	1.06.02.03	1.06.02.03.04	Roof Drainage
1.06	1.06.02	1.06.02.03	1.06.02.03.05	Roof Lights, Skylights and Openings
1.06	1.06.02	1.06.02.03	1.06.02.03.06	Roof Features
1.06	1.06.02	1.06.02.04		**Stairs and Ramps**
1.06	1.06.02	1.06.02.04	1.06.02.04.01	Stair / Ramp Structures
1.06	1.06.02	1.06.02.04	1.06.02.04.02	Stair / Ramp Finishes
1.06	1.06.02	1.06.02.04	1.06.02.04.03	Stair / Ramp Balustrades and Handrails
1.06	1.06.02	1.06.02.04	1.06.02.04.04	Ladders / Chutes / Slides
1.06	1.06.02	1.06.02.05		**External Walls**
1.06	1.06.02	1.06.02.05	1.06.02.05.01	External Enclosing Walls above Ground Level
1.06	1.06.02	1.06.02.05	1.06.02.05.02	External Enclosing Walls below Ground Level
1.06	1.06.02	1.06.02.05	1.06.02.05.03	Solar / Rain Screening
1.06	1.06.02	1.06.02.05	1.06.02.05.04	External Soffits
1.06	1.06.02	1.06.02.05	1.06.02.05.05	Subsidiary Walls, Balustrades and Proprietary Balconies
1.06	1.06.02	1.06.02.05	1.06.02.05.06	Façade Access / Cleaning Systems
1.06	1.06.02	1.06.02.06		**Windows and External Doors**
1.06	1.06.02	1.06.02.06	1.06.02.06.01	External Windows
1.06	1.06.02	1.06.02.06	1.06.02.06.02	External Doors
1.06	1.06.02	1.06.02.07		**Internal Walls and Partitions**
1.06	1.06.02	1.06.02.07	1.06.02.07.01	Walls and Partitions
1.06	1.06.02	1.06.02.07	1.06.02.07.02	Balustrades and Handrails
1.06	1.06.02	1.06.02.07	1.06.02.07.03	Moveable Room Dividers
1.06	1.06.02	1.06.02.07	1.06.02.07.04	Cubicles
1.06	1.06.02	1.06.02.08		**Internal Doors**
1.06	1.06.02	1.06.02.08	1.06.02.08.01	Internal Doors
1.06	1.06.03			**Internal Finishes**
1.06	1.06.03	1.06.03.01		**Wall Finishes**
1.06	1.06.03	1.06.03.01	1.06.03.01.01	Wall Finishes
1.06	1.06.03	1.06.03.02		**Floor Finishes**
1.06	1.06.03	1.06.03.02	1.06.03.02.01	Finishes to Floors
1.06	1.06.03	1.06.03.02	1.06.03.02.02	Raised Access Floors
1.06	1.06.03	1.06.03.03		**Ceiling Finishes**
1.06	1.06.03	1.06.03.03	1.06.03.03.01	Finishes to Ceilings

1.06	1.06.03	1.06.03.03	1.06.03.03.02	False Ceilings
1.06	1.06.03	1.06.03.03	1.06.03.03.03	Demountable Suspended Ceilings
1.06	1.06.04			**Fittings, Furnishings and Equipment**
1.06	1.06.04	1.06.04.01		**Fittings, Furnishings and Equipment**
1.06	1.06.04	1.06.04.01	1.06.04.01.01	General Fittings, Furnishings and Equipment
1.06	1.06.04	1.06.04.01	1.06.04.01.02	Domestic Kitchen Fittings and Equipment
1.06	1.06.04	1.06.04.01	1.06.04.01.03	Special Purpose Fittings, Furnishings and Equipment
1.06	1.06.04	1.06.04.01	1.06.04.01.04	Signs / Notices
1.06	1.06.04	1.06.04.01	1.06.04.01.05	Works of Art
1.06	1.06.04	1.06.04.01	1.06.04.01.06	Non-mechanical and Non-electrical Equipment
1.06	1.06.04	1.06.04.01	1.06.04.01.07	Internal Planting
1.06	1.06.04	1.06.04.01	1.06.04.01.08	Bird and Vermin Control
1.06	1.06.05			**Services to Buildings**
1.06	1.06.05	1.06.05.01		**Sanitary Installations**
1.06	1.06.05	1.06.05.01	1.06.05.01.01	Sanitary Appliances
1.06	1.06.05	1.06.05.01	1.06.05.01.02	Sanitary Ancillaries
1.06	1.06.05	1.06.05.02		**Services Equipment**
1.06	1.06.05	1.06.05.02	1.06.05.02.01	Services Equipment
1.06	1.06.05	1.06.05.03		**Disposal Installations**
1.06	1.06.05	1.06.05.03	1.06.05.03.01	Foul Drainage Above Ground
1.06	1.06.05	1.06.05.03	1.06.05.03.02	Chemical, Toxic and Industrial Waste Drainage
1.06	1.06.05	1.06.05.03	1.06.05.03.03	Refuse Disposal
1.06	1.06.05	1.06.05.04		**Water Installations**
1.06	1.06.05	1.06.05.04	1.06.05.04.01	Mains Water Supply
1.06	1.06.05	1.06.05.04	1.06.05.04.02	Cold Water Distribution
1.06	1.06.05	1.06.05.04	1.06.05.04.03	Hot Water Distribution
1.06	1.06.05	1.06.05.04	1.06.05.04.04	Local Hot Water Distribution
1.06	1.06.05	1.06.05.04	1.06.05.04.05	Steam and Condensate Distribution
1.06	1.06.05	1.06.05.05		**Heat Source**
1.06	1.06.05	1.06.05.05	1.06.05.05.01	Heat Source
1.06	1.06.05	1.06.05.06		**Space Heating & Air Conditioning**
1.06	1.06.05	1.06.05.06	1.06.05.06.01	Central Heating
1.06	1.06.05	1.06.05.06	1.06.05.06.02	Local Heating
1.06	1.06.05	1.06.05.06	1.06.05.06.03	Central Cooling
1.06	1.06.05	1.06.05.06	1.06.05.06.04	Local Cooling
1.06	1.06.05	1.06.05.06	1.06.05.06.05	Central Heating and Cooling
1.06	1.06.05	1.06.05.06	1.06.05.06.06	Local Heating and Cooling
1.06	1.06.05	1.06.05.06	1.06.05.06.07	Central Air Conditioning
1.06	1.06.05	1.06.05.06	1.06.05.06.08	Local Air Conditioning
1.06	1.06.05	1.06.05.07		**Ventilation**
1.06	1.06.05	1.06.05.07	1.06.05.07.01	Central Ventilation
1.06	1.06.05	1.06.05.07	1.06.05.07.02	Local and Special Ventilation
1.06	1.06.05	1.06.05.07	1.06.05.07.03	Smoke Extract / Control
1.06	1.06.05	1.06.05.08		**Electrical Installations**
1.06	1.06.05	1.06.05.08	1.06.05.08.01	Electrical Mains and Sub-mains Distribution
1.06	1.06.05	1.06.05.08	1.06.05.08.02	Power Installations
1.06	1.06.05	1.06.05.08	1.06.05.08.03	Lighting Installations
1.06	1.06.05	1.06.05.08	1.06.05.08.04	Specialist Lighting Installations
1.06	1.06.05	1.06.05.08	1.06.05.08.05	Local Electricity Generation Systems
1.06	1.06.05	1.06.05.08	1.06.05.08.06	Earthing and Bonding Systems
1.06	1.06.05	1.06.05.09		**Fuel Installations**
1.06	1.06.05	1.06.05.09	1.06.05.09.01	Fuel Storage
1.06	1.06.05	1.06.05.09	1.06.05.09.02	Fuel Distribution Systems
1.06	1.06.05	1.06.05.10		**Lift and Conveyor Installations**
1.06	1.06.05	1.06.05.10	1.06.05.10.01	Lifts and Enclosed Hoists
1.06	1.06.05	1.06.05.10	1.06.05.10.02	Escalators
1.06	1.06.05	1.06.05.10	1.06.05.10.03	Moving Pavements
1.06	1.06.05	1.06.05.10	1.06.05.10.04	Powered Stair lifts
1.06	1.06.05	1.06.05.10	1.06.05.10.05	Conveyors

1.06	1.06.05	1.06.05.10	1.06.05.10.06	Dock Levellers and Scissor Lifts
1.06	1.06.05	1.06.05.10	1.06.05.10.08	Car Lifts, Car Stacking Systems, Turntables and the like
1.06	1.06.05	1.06.05.10	1.06.05.10.09	Document Handling Systems
1.06	1.06.05	1.06.05.10	1.06.05.10.10	Other Lift and Conveyor Systems
1.06	1.06.05	1.06.05.11		**Fire and Lightning Protection**
1.06	1.06.05	1.06.05.11	1.06.05.11.01	Fire Fighting Systems
1.06	1.06.05	1.06.05.11	1.06.05.11.02	Fire Suppression Systems
1.06	1.06.05	1.06.05.11	1.06.05.11.03	Lightning Protection
1.06	1.06.05	1.06.05.12		**Control Systems**
1.06	1.06.05	1.06.05.12	1.06.05.12.01	Central Control / Building Management Systems
1.06	1.06.05	1.06.05.13		**Special Installations**
1.06	1.06.05	1.06.05.13	1.06.05.13.01	Specialist Piped Supply Installation
1.06	1.06.05	1.06.05.13	1.06.05.13.02	Specialist Refrigeration Systems
1.06	1.06.05	1.06.05.13	1.06.05.13.03	Specialist Mechanical Installations
1.06	1.06.05	1.06.05.13	1.06.05.13.04	Specialist Electrical / Electronic Installations
1.06	1.06.05	1.06.05.13	1.06.05.13.05	Water Features
1.06	1.06.05	1.06.05.13	1.06.05.13.06	Specialist Station Equipment
1.06	1.06.05	1.06.05.14		**Builders Work in Connection with Services**
1.06	1.06.05	1.06.05.14	1.06.05.14.01	Builder's Work in Connection with Services
1.06	1.06.06			**Services to Tunnels and Shafts**
1.06	1.06.06	1.06.06.01		**Sanitary Installations**
1.06	1.06.06	1.06.06.01	1.06.06.01.01	Sanitary Appliances
1.06	1.06.06	1.06.06.01	1.06.06.01.02	Sanitary Ancillaries
1.06	1.06.06	1.06.06.02		**Services Equipment**
1.06	1.06.06	1.06.06.02	1.06.06.02.01	Services Equipment
1.06	1.06.06	1.06.06.03		**Disposal Installations**
1.06	1.06.06	1.06.06.03	1.06.06.03.01	Foul Drainage Above Ground
1.06	1.06.06	1.06.06.03	1.06.06.03.02	Chemical, Toxic and Industrial Waste Drainage
1.06	1.06.06	1.06.06.03	1.06.06.03.03	Refuse Disposal
1.06	1.06.06	1.06.06.04		**Water Installations**
1.06	1.06.06	1.06.06.04	1.06.06.04.01	Mains Water Supply
1.06	1.06.06	1.06.06.04	1.06.06.04.02	Cold Water Distribution
1.06	1.06.06	1.06.06.04	1.06.06.04.03	Hot Water Distribution
1.06	1.06.06	1.06.06.04	1.06.06.04.04	Local Hot Water Distribution
1.06	1.06.06	1.06.06.04	1.06.06.04.05	Steam and Condensate Distribution
1.06	1.06.06	1.06.06.05		**Heat Source**
1.06	1.06.06	1.06.06.05	1.06.06.05.01	Heat Source
1.06	1.06.06	1.06.06.06		**Space Heating and Air Conditioning**
1.06	1.06.06	1.06.06.06	1.06.06.06.01	Central Heating
1.06	1.06.06	1.06.06.06	1.06.06.06.02	Local Heating
1.06	1.06.06	1.06.06.06	1.06.06.06.03	Central Cooling
1.06	1.06.06	1.06.06.06	1.06.06.06.04	Local Cooling
1.06	1.06.06	1.06.06.06	1.06.06.06.05	Central Heating and Cooling
1.06	1.06.06	1.06.06.06	1.06.06.06.06	Local Heating and Cooling
1.06	1.06.06	1.06.06.06	1.06.06.06.07	Central Air Conditioning
1.06	1.06.06	1.06.06.06	1.06.06.06.08	Local Air Conditioning
1.06	1.06.06	1.06.06.07		**Ventilation**
1.06	1.06.06	1.06.06.07	1.06.06.07.01	Central Ventilation
1.06	1.06.06	1.06.06.07	1.06.06.07.02	Local and Special Ventilation
1.06	1.06.06	1.06.06.07	1.06.06.07.03	Smoke Extract / Control
1.06	1.06.06	1.06.06.08		**Electrical Installations**
1.06	1.06.06	1.06.06.08	1.06.06.08.01	Electrical Mains and Sub-mains Distribution
1.06	1.06.06	1.06.06.08	1.06.06.08.02	Power Installations
1.06	1.06.06	1.06.06.08	1.06.06.08.03	Lighting Installations
1.06	1.06.06	1.06.06.08	1.06.06.08.04	Specialist Lighting Installations
1.06	1.06.06	1.06.06.08	1.06.06.08.05	Local Electricity Generation Systems
1.06	1.06.06	1.06.06.08	1.06.06.08.06	Earthing and Bonding Systems
1.06	1.06.06	1.06.06.09		**Fuel Installations**
1.06	1.06.06	1.06.06.09	1.06.06.09.01	Fuel Storage

1.06	1.06.06	1.06.06.09	1.06.06.09.02	Fuel Distribution Systems
1.06	1.06.06	1.06.06.10		**Lift and Conveyor Installations**
1.06	1.06.06	1.06.06.10	1.06.06.10.01	Lifts and Enclosed Hoists
1.06	1.06.06	1.06.06.10	1.06.06.10.02	Escalators
1.06	1.06.06	1.06.06.10	1.06.06.10.03	Moving Pavements
1.06	1.06.06	1.06.06.10	1.06.06.10.04	Powered Stair lifts
1.06	1.06.06	1.06.06.10	1.06.06.10.05	Conveyors
1.06	1.06.06	1.06.06.10	1.06.06.10.06	Dock Levellers and Scissor Lifts
1.06	1.06.06	1.06.06.10	1.06.06.10.07	Cranes and Unenclosed Hoists
1.06	1.06.06	1.06.06.10	1.06.06.10.08	Car Lifts, Car Stacking Systems, Turntables and the like
1.06	1.06.06	1.06.06.10	1.06.06.10.09	Document Handling Systems
1.06	1.06.06	1.06.06.10	1.06.06.10.10	Other Lift and Conveyor Systems
1.06	1.06.06	1.06.06.11		**Fire and Lightning Protection**
1.06	1.06.06	1.06.06.11	1.06.06.11.01	Fire Fighting Systems
1.06	1.06.06	1.06.06.11	1.06.06.11.02	Fire Suppression Systems
1.06	1.06.06	1.06.06.11	1.06.06.11.03	Lightning Protection
1.06	1.06.06	1.06.06.12		**Control Systems**
1.06	1.06.06	1.06.06.12	1.06.06.12.01	Central Control / Building Management Systems
1.06	1.06.06	1.06.06.13		**Special Installations**
1.06	1.06.06	1.06.06.13	1.06.06.13.01	Specialist Piped Supply Installation
1.06	1.06.06	1.06.06.13	1.06.06.13.02	Specialist Refrigeration Systems
1.06	1.06.06	1.06.06.13	1.06.06.13.03	Specialist Mechanical Installations
1.06	1.06.06	1.06.06.13	1.06.06.13.04	Specialist Electrical / Electronic Installations
1.06	1.06.06	1.06.06.13	1.06.06.13.05	Water Features
1.06	1.06.06	1.06.06.13	1.06.06.13.06	Specialist Station Equipment
1.06	1.06.06	1.06.06.14		**Builders Work in Connection with Services**
1.06	1.06.06	1.06.06.14	1.06.06.14.01	Builder's Work in Connection with Services
1.06	1.06.07			**Services to Subways and Underpasses**
1.06	1.06.07	1.06.07.01		**Sanitary Installations**
1.06	1.06.07	1.06.07.01	1.06.07.01.01	Sanitary Appliances
1.06	1.06.07	1.06.07.01	1.06.07.01.02	Sanitary Ancillaries
1.06	1.06.07	1.06.07.02		**Services Equipment**
1.06	1.06.07	1.06.07.02	1.06.07.02.01	Services Equipment
1.06	1.06.07	1.06.07.03		**Disposal Installations**
1.06	1.06.07	1.06.07.03	1.06.07.03.01	Foul Drainage Above Ground
1.06	1.06.07	1.06.07.03	1.06.07.03.02	Chemical, Toxic and Industrial Waste Drainage
1.06	1.06.07	1.06.07.03	1.06.07.03.03	Refuse Disposal
1.06	1.06.07	1.06.07.04		**Water Installations**
1.06	1.06.07	1.06.07.04	1.06.07.04.01	Mains Water Supply
1.06	1.06.07	1.06.07.04	1.06.07.04.02	Cold Water Distribution
1.06	1.06.07	1.06.07.04	1.06.07.04.03	Hot Water Distribution
1.06	1.06.07	1.06.07.04	1.06.07.04.04	Local Hot Water Distribution
1.06	1.06.07	1.06.07.04	1.06.07.04.05	Steam and Condensate Distribution
1.06	1.06.07	1.06.07.05		**Heat Source**
1.06	1.06.07	1.06.07.05	1.06.07.05.01	Heat Source
1.06	1.06.07	1.06.07.06		**Space Heating and Air Conditioning**
1.06	1.06.07	1.06.07.06	1.06.07.06.01	Central Heating
1.06	1.06.07	1.06.07.06	1.06.07.06.02	Local Heating
1.06	1.06.07	1.06.07.06	1.06.07.06.03	Central Cooling
1.06	1.06.07	1.06.07.06	1.06.07.06.04	Local Cooling
1.06	1.06.07	1.06.07.06	1.06.07.06.05	Central Heating and Cooling
1.06	1.06.07	1.06.07.06	1.06.07.06.06	Local Heating and Cooling
1.06	1.06.07	1.06.07.06	1.06.07.06.07	Central Air Conditioning
1.06	1.06.07	1.06.07.06	1.06.07.06.08	Local Air Conditioning
1.06	1.06.07	1.06.07.07		**Ventilation**
1.06	1.06.07	1.06.07.07	1.06.07.07.01	Central Ventilation
1.06	1.06.07	1.06.07.07	1.06.07.07.02	Local and Special Ventilation
1.06	1.06.07	1.06.07.07	1.06.07.07.03	Smoke Extract / Control
1.06	1.06.07	1.06.07.08		**Electrical Installations**

1.06	1.06.07	1.06.07.08	1.06.07.08.01	Electrical Mains and Sub-mains Distribution
1.06	1.06.07	1.06.07.08	1.06.07.08.02	Power Installations
1.06	1.06.07	1.06.07.08	1.06.07.08.03	Lighting Installations
1.06	1.06.07	1.06.07.08	1.06.07.08.04	Specialist Lighting Installations
1.06	1.06.07	1.06.07.08	1.06.07.08.05	Local Electricity Generation Systems
1.06	1.06.07	1.06.07.08	1.06.07.08.06	Earthing and Bonding Systems
1.06	1.06.07	1.06.07.09		**Fuel Installations**
1.06	1.06.07	1.06.07.09	1.06.07.09.01	Fuel Storage
1.06	1.06.07	1.06.07.09	1.06.07.09.02	Fuel Distribution Systems
1.06	1.06.07	1.06.07.10		**Lift and Conveyor Installations**
1.06	1.06.07	1.06.07.10	1.06.07.10.01	Lifts and Enclosed Hoists
1.06	1.06.07	1.06.07.10	1.06.07.10.02	Escalators
1.06	1.06.07	1.06.07.10	1.06.07.10.03	Moving Pavements
1.06	1.06.07	1.06.07.10	1.06.07.10.04	Powered Stair lifts
1.06	1.06.07	1.06.07.10	1.06.07.10.05	Conveyors
1.06	1.06.07	1.06.07.10	1.06.07.10.06	Dock Levellers and Scissor Lifts
1.06	1.06.07	1.06.07.10	1.06.07.10.07	Cranes and Unenclosed Hoists
1.06	1.06.07	1.06.07.10	1.06.07.10.08	Car Lifts, Car Stacking Systems, Turntables and the like
1.06	1.06.07	1.06.07.10	1.06.07.10.09	Document Handling Systems
1.06	1.06.07	1.06.07.10	1.06.07.10.10	Other Lift and Conveyor Systems
1.06	1.06.07	1.06.07.11		**Fire and Lightning Protection**
1.06	1.06.07	1.06.07.11	1.06.07.11.01	Fire Fighting Systems
1.06	1.06.07	1.06.07.11	1.06.07.11.02	Fire Suppression Systems
1.06	1.06.07	1.06.07.11	1.06.07.11.03	Lightning Protection
1.06	1.06.07	1.06.07.12		**Control Systems**
1.06	1.06.07	1.06.07.12	1.06.07.12.01	Central Control / Building Management Systems
1.06	1.06.07	1.06.07.13		**Special Installations**
1.06	1.06.07	1.06.07.13	1.06.07.13.01	Specialist Piped Supply Installation
1.06	1.06.07	1.06.07.13	1.06.07.13.02	Specialist Refrigeration Systems
1.06	1.06.07	1.06.07.13	1.06.07.13.03	Specialist Mechanical Installations
1.06	1.06.07	1.06.07.13	1.06.07.13.04	Specialist Electrical / Electronic Installations
1.06	1.06.07	1.06.07.13	1.06.07.13.05	Water Features
1.06	1.06.07	1.06.07.13	1.06.07.13.06	Specialist Station Equipment
1.06	1.06.07	1.06.07.14		**Builders Work in Connection with Services**
1.06	1.06.07	1.06.07.14	1.06.07.14.01	Builder's Work in Connection with Services
1.06	1.06.08			**Services to Bridges and Viaducts for Road and Rail Vehicles**
1.06	1.06.08	1.06.08.01		**Sanitary Installations**
1.06	1.06.08	1.06.08.01	1.06.08.01.01	Sanitary Appliances
1.06	1.06.08	1.06.08.01	1.06.08.01.02	Sanitary Ancillaries
1.06	1.06.08	1.06.08.02		**Services Equipment**
1.06	1.06.08	1.06.08.02	1.06.08.02.01	Services Equipment
1.06	1.06.08	1.06.08.03		**Disposal Installations**
1.06	1.06.08	1.06.08.03	1.06.08.03.01	Foul Drainage Above Ground
1.06	1.06.08	1.06.08.03	1.06.08.03.02	Chemical, Toxic and Industrial Waste Drainage
1.06	1.06.08	1.06.08.03	1.06.08.03.03	Refuse Disposal
1.06	1.06.08	1.06.08.04		**Water Installations**
1.06	1.06.08	1.06.08.04	1.06.08.04.01	Mains Water Supply
1.06	1.06.08	1.06.08.04	1.06.08.04.02	Cold Water Distribution
1.06	1.06.08	1.06.08.04	1.06.08.04.03	Hot Water Distribution
1.06	1.06.08	1.06.08.04	1.06.08.04.04	Local Hot Water Distribution
1.06	1.06.08	1.06.08.04	1.06.08.04.05	Steam and Condensate Distribution
1.06	1.06.08	1.06.08.05		**Heat Source**
1.06	1.06.08	1.06.08.05	1.06.08.05.01	Heat Source
1.06	1.06.08	1.06.08.06		**Space Heating and Air Conditioning**
1.06	1.06.08	1.06.08.06	1.06.08.06.01	Central Heating
1.06	1.06.08	1.06.08.06	1.06.08.06.02	Local Heating
1.06	1.06.08	1.06.08.06	1.06.08.06.03	Central Cooling
1.06	1.06.08	1.06.08.06	1.06.08.06.04	Local Cooling
1.06	1.06.08	1.06.08.06	1.06.08.06.05	Central Heating and Cooling

1.06	1.06.08	1.06.08.06	1.06.08.06.06	Local Heating and Cooling
1.06	1.06.08	1.06.08.06	1.06.08.06.07	Central Air Conditioning
1.06	1.06.08	1.06.08.06	1.06.08.06.08	Local Air Conditioning
1.06	1.06.08	1.06.08.07		**Ventilation**
1.06	1.06.08	1.06.08.07	1.06.08.07.01	Central Ventilation
1.06	1.06.08	1.06.08.07	1.06.08.07.02	Local and Special Ventilation
1.06	1.06.08	1.06.08.07	1.06.08.07.03	Smoke Extract / Control
1.06	1.06.08	1.06.08.08		**Electrical Installations**
1.06	1.06.08	1.06.08.08	1.06.08.08.01	Electrical Mains and Sub-mains Distribution
1.06	1.06.08	1.06.08.08	1.06.08.08.02	Power Installations
1.06	1.06.08	1.06.08.08	1.06.08.08.03	Lighting Installations
1.06	1.06.08	1.06.08.08	1.06.08.08.04	Specialist Lighting Installations
1.06	1.06.08	1.06.08.08	1.06.08.08.05	Local Electricity Generation Systems
1.06	1.06.08	1.06.08.08	1.06.08.08.06	Earthing and Bonding Systems
1.06	1.06.08	1.06.08.09		**Fuel Installations**
1.06	1.06.08	1.06.08.09	1.06.08.09.01	Fuel Storage
1.06	1.06.08	1.06.08.09	1.06.08.09.02	Fuel Distribution Systems
1.06	1.06.08	1.06.08.10		**Lift and Conveyor Installations**
1.06	1.06.08	1.06.08.10	1.06.08.10.01	Lifts and Enclosed Hoists
1.06	1.06.08	1.06.08.10	1.06.08.10.02	Escalators
1.06	1.06.08	1.06.08.10	1.06.08.10.03	Moving Pavements
1.06	1.06.08	1.06.08.10	1.06.08.10.04	Powered Stair lifts
1.06	1.06.08	1.06.08.10	1.06.08.10.05	Conveyors
1.06	1.06.08	1.06.08.10	1.06.08.10.06	Dock Levellers and Scissor Lifts
1.06	1.06.08	1.06.08.10	1.06.08.10.07	Cranes and Unenclosed Hoists
1.06	1.06.08	1.06.08.10	1.06.08.10.08	Car Lifts, Car Stacking Systems, Turntables and the like
1.06	1.06.08	1.06.08.10	1.06.08.10.09	Document Handling Systems
1.06	1.06.08	1.06.08.10	1.06.08.10.10	Other Lift and Conveyor Systems
1.06	1.06.08	1.06.08.11		**Fire and Lightning Protection**
1.06	1.06.08	1.06.08.11	1.06.08.11.01	Fire Fighting Systems
1.06	1.06.08	1.06.08.11	1.06.08.11.02	Fire Suppression Systems
1.06	1.06.08	1.06.08.11	1.06.08.11.03	Lightning Protection
1.06	1.06.08	1.06.08.12		**Control Systems**
1.06	1.06.08	1.06.08.12	1.06.08.12.01	Central Control / Building Management Systems
1.06	1.06.08	1.06.08.13		**Special Installations**
1.06	1.06.08	1.06.08.13	1.06.08.13.01	Specialist Piped Supply Installation
1.06	1.06.08	1.06.08.13	1.06.08.13.02	Specialist Refrigeration Systems
1.06	1.06.08	1.06.08.13	1.06.08.13.03	Specialist Mechanical Installations
1.06	1.06.08	1.06.08.13	1.06.08.13.04	Specialist Electrical / Electronic Installations
1.06	1.06.08	1.06.08.13	1.06.08.13.05	Water Features
1.06	1.06.08	1.06.08.13	1.06.08.13.06	Specialist Station Equipment
1.06	1.06.08	1.06.08.14		**Builders Work in Connection with Services**
1.06	1.06.08	1.06.08.14	1.06.08.14.01	Builder's Work in Connection with Services
1.06	1.06.09			**Services to Footbridges**
1.06	1.06.09	1.06.09.01		**Sanitary Installations**
1.06	1.06.09	1.06.09.01	1.06.09.01.01	Sanitary Appliances
1.06	1.06.09	1.06.09.01	1.06.09.01.02	Sanitary Ancillaries
1.06	1.06.09	1.06.09.02		**Services Equipment**
1.06	1.06.09	1.06.09.02	1.06.09.02.01	Services Equipment
1.06	1.06.09	1.06.09.03		**Disposal Installations**
1.06	1.06.09	1.06.09.03	1.06.09.03.01	Foul Drainage Above Ground
1.06	1.06.09	1.06.09.03	1.06.09.03.02	Chemical, Toxic and Industrial Waste Drainage
1.06	1.06.09	1.06.09.03	1.06.09.03.03	Refuse Disposal
1.06	1.06.09	1.06.09.04		**Water Installations**
1.06	1.06.09	1.06.09.04	1.06.09.04.01	Mains Water Supply
1.06	1.06.09	1.06.09.04	1.06.09.04.02	Cold Water Distribution
1.06	1.06.09	1.06.09.04	1.06.09.04.03	Hot Water Distribution
1.06	1.06.09	1.06.09.04	1.06.09.04.04	Local Hot Water Distribution
1.06	1.06.09	1.06.09.04	1.06.09.04.05	Steam and Condensate Distribution

1.06	1.06.09	1.06.09.05		**Heat Source**
1.06	1.06.09	1.06.09.05	1.06.09.05.01	Heat Source
1.06	1.06.09	1.06.09.06		**Space Heating and Air Conditioning**
1.06	1.06.09	1.06.09.06	1.06.09.06.01	Central Heating
1.06	1.06.09	1.06.09.06	1.06.09.06.02	Local Heating
1.06	1.06.09	1.06.09.06	1.06.09.06.03	Central Cooling
1.06	1.06.09	1.06.09.06	1.06.09.06.04	Local Cooling
1.06	1.06.09	1.06.09.06	1.06.09.06.05	Central Heating and Cooling
1.06	1.06.09	1.06.09.06	1.06.09.06.06	Local Heating and Cooling
1.06	1.06.09	1.06.09.06	1.06.09.06.07	Central Air Conditioning
1.06	1.06.09	1.06.09.06	1.06.09.06.08	Local Air Conditioning
1.06	1.06.09	1.06.09.07		**Ventilation**
1.06	1.06.09	1.06.09.07	1.06.09.07.01	Central Ventilation
1.06	1.06.09	1.06.09.07	1.06.09.07.02	Local and Special Ventilation
1.06	1.06.09	1.06.09.07	1.06.09.07.03	Smoke Extract / Control
1.06	1.06.09	1.06.09.08		**Electrical Installations**
1.06	1.06.09	1.06.09.08	1.06.09.08.01	Electrical Mains and Sub-mains Distribution
1.06	1.06.09	1.06.09.08	1.06.09.08.02	Power Installations
1.06	1.06.09	1.06.09.08	1.06.09.08.03	Lighting Installations
1.06	1.06.09	1.06.09.08	1.06.09.08.04	Specialist Lighting Installations
1.06	1.06.09	1.06.09.08	1.06.09.08.05	Local Electricity Generation Systems
1.06	1.06.09	1.06.09.08	1.06.09.08.06	Earthing and Bonding Systems
1.06	1.06.09	1.06.09.09		**Fuel Installations**
1.06	1.06.09	1.06.09.09	1.06.09.09.01	Fuel Storage
1.06	1.06.09	1.06.09.09	1.06.09.09.02	Fuel Distribution Systems
1.06	1.06.09	1.06.09.10		**Lift and Conveyor Installations**
1.06	1.06.09	1.06.09.10	1.06.09.10.01	Lifts and Enclosed Hoists
1.06	1.06.09	1.06.09.10	1.06.09.10.02	Escalators
1.06	1.06.09	1.06.09.10	1.06.09.10.03	Moving Pavements
1.06	1.06.09	1.06.09.10	1.06.09.10.04	Powered Stair lifts
1.06	1.06.09	1.06.09.10	1.06.09.10.05	Conveyors
1.06	1.06.09	1.06.09.10	1.06.09.10.06	Dock Levellers and Scissor Lifts
1.06	1.06.09	1.06.09.10	1.06.09.10.07	Cranes and Unenclosed Hoists
1.06	1.06.09	1.06.09.10	1.06.09.10.08	Car Lifts, Car Stacking Systems, Turntables and the like
1.06	1.06.09	1.06.09.10	1.06.09.10.09	Document Handling Systems
1.06	1.06.09	1.06.09.10	1.06.09.10.10	Other Lift and Conveyor Systems
1.06	1.06.09	1.06.09.11		**Fire and Lightning Protection**
1.06	1.06.09	1.06.09.11	1.06.09.11.01	Fire Fighting Systems
1.06	1.06.09	1.06.09.11	1.06.09.11.02	Fire Suppression Systems
1.06	1.06.09	1.06.09.11	1.06.09.11.03	Lightning Protection
1.06	1.06.09	1.06.09.12		**Control Systems**
1.06	1.06.09	1.06.09.12	1.06.09.12.01	Central Control / Building Management Systems
1.06	1.06.09	1.06.09.13		**Special Installations**
1.06	1.06.09	1.06.09.13	1.06.09.13.01	Specialist Piped Supply Installation
1.06	1.06.09	1.06.09.13	1.06.09.13.02	Specialist Refrigeration Systems
1.06	1.06.09	1.06.09.13	1.06.09.13.03	Specialist Mechanical Installations
1.06	1.06.09	1.06.09.13	1.06.09.13.04	Specialist Electrical / Electronic Installations
1.06	1.06.09	1.06.09.13	1.06.09.13.05	Water Features
1.06	1.06.09	1.06.09.13	1.06.09.13.06	Specialist Station Equipment
1.06	1.06.09	1.06.09.14		**Builders Work in Connection with Services**
1.06	1.06.09	1.06.09.14	1.06.09.14.01	Builder's Work in Connection with Services
1.06	1.06.10			**Services to Platforms**
1.06	1.06.10	1.06.10.01		**Sanitary Installations**
1.06	1.06.10	1.06.10.01	1.06.10.01.01	Sanitary Appliances
1.06	1.06.10	1.06.10.01	1.06.10.01.02	Sanitary Ancillaries
1.06	1.06.10	1.06.10.02		**Services Equipment**
1.06	1.06.10	1.06.10.02	1.06.10.02.01	Services Equipment
1.06	1.06.10	1.06.10.03		**Disposal Installations**
1.06	1.06.10	1.06.10.03	1.06.10.03.01	Foul Drainage Above Ground

1.06	1.06.10	1.06.10.03	1.06.10.03.02	Chemical, Toxic and Industrial Waste Drainage
1.06	1.06.10	1.06.10.03	1.06.10.03.03	Refuse Disposal
1.06	1.06.10	1.06.10.04		**Water Installations**
1.06	1.06.10	1.06.10.04	1.06.10.04.01	Mains Water Supply
1.06	1.06.10	1.06.10.04	1.06.10.04.02	Cold Water Distribution
1.06	1.06.10	1.06.10.04	1.06.10.04.03	Hot Water Distribution
1.06	1.06.10	1.06.10.04	1.06.10.04.04	Local Hot Water Distribution
1.06	1.06.10	1.06.10.04	1.06.10.04.05	Steam and Condensate Distribution
1.06	1.06.10	1.06.10.05		**Heat Source**
1.06	1.06.10	1.06.10.05	1.06.10.05.01	Heat Source
1.06	1.06.10	1.06.10.06		**Space Heating & Air Conditioning**
1.06	1.06.10	1.06.10.06	1.06.10.06.01	Central Heating
1.06	1.06.10	1.06.10.06	1.06.10.06.02	Local Heating
1.06	1.06.10	1.06.10.06	1.06.10.06.03	Central Cooling
1.06	1.06.10	1.06.10.06	1.06.10.06.04	Local Cooling
1.06	1.06.10	1.06.10.06	1.06.10.06.05	Central Heating and Cooling
1.06	1.06.10	1.06.10.06	1.06.10.06.06	Local Heating and Cooling
1.06	1.06.10	1.06.10.06	1.06.10.06.07	Central Air Conditioning
1.06	1.06.10	1.06.10.06	1.06.10.06.08	Local Air Conditioning
1.06	1.06.10	1.06.10.07		**Ventilation**
1.06	1.06.10	1.06.10.07	1.06.10.07.01	Central Ventilation
1.06	1.06.10	1.06.10.07	1.06.10.07.02	Local and Special Ventilation
1.06	1.06.10	1.06.10.07	1.06.10.07.03	Smoke Extract / Control
1.06	1.06.10	1.06.10.08		**Electrical Installations**
1.06	1.06.10	1.06.10.08	1.06.10.08.01	Electrical Mains and Sub-mains Distribution
1.06	1.06.10	1.06.10.08	1.06.10.08.02	Power Installations
1.06	1.06.10	1.06.10.08	1.06.10.08.03	Lighting Installations
1.06	1.06.10	1.06.10.08	1.06.10.08.04	Specialist Lighting Installations
1.06	1.06.10	1.06.10.08	1.06.10.08.05	Local Electricity Generation Systems
1.06	1.06.10	1.06.10.08	1.06.10.08.06	Earthing and Bonding Systems
1.06	1.06.10	1.06.10.09		**Fuel Installations**
1.06	1.06.10	1.06.10.09	1.06.10.09.01	Fuel Storage
1.06	1.06.10	1.06.10.09	1.06.10.09.02	Fuel Distribution Systems
1.06	1.06.10	1.06.10.10		**Lift and Conveyor Installations**
1.06	1.06.10	1.06.10.10	1.06.10.10.01	Lifts and Enclosed Hoists
1.06	1.06.10	1.06.10.10	1.06.10.10.02	Escalators
1.06	1.06.10	1.06.10.10	1.06.10.10.03	Moving Pavements
1.06	1.06.10	1.06.10.10	1.06.10.10.04	Powered Stair lifts
1.06	1.06.10	1.06.10.10	1.06.10.10.05	Conveyors
1.06	1.06.10	1.06.10.10	1.06.10.10.06	Dock Levellers and Scissor Lifts
1.06	1.06.10	1.06.10.10	1.06.10.10.07	Cranes and Unenclosed Hoists
1.06	1.06.10	1.06.10.10	1.06.10.10.08	Car Lifts, Car Stacking Systems, Turntables and the like
1.06	1.06.10	1.06.10.10	1.06.10.10.09	Document Handling Systems
1.06	1.06.10	1.06.10.10	1.06.10.10.10	Other Lift and Conveyor Systems
1.06	1.06.10	1.06.10.11		**Fire and Lightning Protection**
1.06	1.06.10	1.06.10.11	1.06.10.11.01	Fire Fighting Systems
1.06	1.06.10	1.06.10.11	1.06.10.11.02	Fire Suppression Systems
1.06	1.06.10	1.06.10.11	1.06.10.11.03	Lightning Protection
1.06	1.06.10	1.06.10.12		**Control Systems**
1.06	1.06.10	1.06.10.12	1.06.10.12.01	Central Control / Building Management Systems
1.06	1.06.10	1.06.10.13		**Special Installations**
1.06	1.06.10	1.06.10.13	1.06.10.13.01	Specialist Piped Supply Installation
1.06	1.06.10	1.06.10.13	1.06.10.13.02	Specialist Refrigeration Systems
1.06	1.06.10	1.06.10.13	1.06.10.13.03	Specialist Mechanical Installations
1.06	1.06.10	1.06.10.13	1.06.10.13.04	Specialist Electrical / Electronic Installations
1.06	1.06.10	1.06.10.13	1.06.10.13.05	Water Features
1.06	1.06.10	1.06.10.13	1.06.10.13.06	Specialist Station Equipment
1.06	1.06.10	1.06.10.14		**Builders Work in Connection with Services**
1.06	1.06.10	1.06.10.14	1.06.10.14.01	Builder's Work in Connection with Services

1.06	1.06.11			**Services to Other Structures (stated)**
1.06	1.06.11	1.06.11.01		**Sanitary Installations**
1.06	1.06.11	1.06.11.01	1.06.11.01.01	Sanitary Appliances
1.06	1.06.11	1.06.11.01	1.06.11.01.02	Sanitary Ancillaries
1.06	1.06.11	1.06.11.02		**Services Equipment**
1.06	1.06.11	1.06.11.02	1.06.11.02.01	Services Equipment
1.06	1.06.11	1.06.11.03		**Disposal Installations**
1.06	1.06.11	1.06.11.03	1.06.11.03.01	Foul Drainage Above Ground
1.06	1.06.11	1.06.11.03	1.06.11.03.02	Chemical, Toxic and Industrial Waste Drainage
1.06	1.06.11	1.06.11.03	1.06.11.03.03	Refuse Disposal
1.06	1.06.11	1.06.11.04		**Water Installations**
1.06	1.06.11	1.06.11.04	1.06.11.04.01	Mains Water Supply
1.06	1.06.11	1.06.11.04	1.06.11.04.02	Cold Water Distribution
1.06	1.06.11	1.06.11.04	1.06.11.04.03	Hot Water Distribution
1.06	1.06.11	1.06.11.04	1.06.11.04.04	Local Hot Water Distribution
1.06	1.06.11	1.06.11.04	1.06.11.04.05	Steam and Condensate Distribution
1.06	1.06.11	1.06.11.05		**Heat Source**
1.06	1.06.11	1.06.11.05	1.06.11.05.01	Heat Source
1.06	1.06.11	1.06.11.06		**Space Heating and Air Conditioning**
1.06	1.06.11	1.06.11.06	1.06.11.06.01	Central Heating
1.06	1.06.11	1.06.11.06	1.06.11.06.02	Local Heating
1.06	1.06.11	1.06.11.06	1.06.11.06.03	Central Cooling
1.06	1.06.11	1.06.11.06	1.06.11.06.04	Local Cooling
1.06	1.06.11	1.06.11.06	1.06.11.06.05	Central Heating and Cooling
1.06	1.06.11	1.06.11.06	1.06.11.06.06	Local Heating and Cooling
1.06	1.06.11	1.06.11.06	1.06.11.06.07	Central Air Conditioning
1.06	1.06.11	1.06.11.06	1.06.11.06.08	Local Air Conditioning
1.06	1.06.11	1.06.11.07		**Ventilation**
1.06	1.06.11	1.06.11.07	1.06.11.07.01	Central Ventilation
1.06	1.06.11	1.06.11.07	1.06.11.07.02	Local and Special Ventilation
1.06	1.06.11	1.06.11.07	1.06.11.07.03	Smoke Extract / Control
1.06	1.06.11	1.06.11.08		**Electrical Installations**
1.06	1.06.11	1.06.11.08	1.06.11.08.01	Electrical Mains and Sub-mains Distribution
1.06	1.06.11	1.06.11.08	1.06.11.08.02	Power Installations
1.06	1.06.11	1.06.11.08	1.06.11.08.03	Lighting Installations
1.06	1.06.11	1.06.11.08	1.06.11.08.04	Specialist Lighting Installations
1.06	1.06.11	1.06.11.08	1.06.11.08.05	Local Electricity Generation Systems
1.06	1.06.11	1.06.11.08	1.06.11.08.06	Earthing and Bonding Systems
1.06	1.06.11	1.06.11.09		**Fuel Installations**
1.06	1.06.11	1.06.11.09	1.06.11.09.01	Fuel Storage
1.06	1.06.11	1.06.11.09	1.06.11.09.02	Fuel Distribution Systems
1.06	1.06.11	1.06.11.10		**Lift and Conveyor Installations**
1.06	1.06.11	1.06.11.10	1.06.11.10.01	Lifts and Enclosed Hoists
1.06	1.06.11	1.06.11.10	1.06.11.10.02	Escalators
1.06	1.06.11	1.06.11.10	1.06.11.10.03	Moving Pavements
1.06	1.06.11	1.06.11.10	1.06.11.10.04	Powered Stair lifts
1.06	1.06.11	1.06.11.10	1.06.11.10.05	Conveyors
1.06	1.06.11	1.06.11.10	1.06.11.10.06	Dock Levellers and Scissor Lifts
1.06	1.06.11	1.06.11.10	1.06.11.10.07	Cranes and Unenclosed Hoists
1.06	1.06.11	1.06.11.10	1.06.11.10.08	Car Lifts, Car Stacking Systems, Turntables and the like
1.06	1.06.11	1.06.11.10	1.06.11.10.09	Document Handling Systems
1.06	1.06.11	1.06.11.10	1.06.11.10.10	Other Lift and Conveyor Systems
1.06	1.06.11	1.06.11.11		**Fire and Lightning Protection**
1.06	1.06.11	1.06.11.11	1.06.11.11.01	Fire Fighting Systems
1.06	1.06.11	1.06.11.11	1.06.11.11.02	Fire Suppression Systems
1.06	1.06.11	1.06.11.11	1.06.11.11.03	Lightning Protection
1.06	1.06.11	1.06.11.12		**Control Systems**
1.06	1.06.11	1.06.11.12	1.06.11.12.01	Central Control / Building Management Systems
1.06	1.06.11	1.06.11.13		**Special Installations**

1.06	1.06.11	1.06.11.13	1.06.11.13.01	Specialist Piped Supply Installation
1.06	1.06.11	1.06.11.13	1.06.11.13.02	Specialist Refrigeration Systems
1.06	1.06.11	1.06.11.13	1.06.11.13.03	Specialist Mechanical Installations
1.06	1.06.11	1.06.11.13	1.06.11.13.04	Specialist Electrical / Electronic Installations
1.06	1.06.11	1.06.11.13	1.06.11.13.05	Water Features
1.06	1.06.11	1.06.11.13	1.06.11.13.06	Specialist Station Equipment
1.06	1.06.11	1.06.11.14		**Builders Work in Connection with Services**
1.06	1.06.11	1.06.11.14	1.06.11.14.01	Builder's Work in Connection with Services
1.06	1.06.12			**External Services**
1.06	1.06.12	1.06.12.01		**External Services**
1.06	1.06.12	1.06.12.01	1.06.12.01.01	Water Mains Supply
1.06	1.06.12	1.06.12.01	1.06.12.01.02	Electricity Mains Supply
1.06	1.06.12	1.06.12.01	1.06.12.01.03	External Transformation Devices
1.06	1.06.12	1.06.12.01	1.06.12.01.04	Electricity Distribution to External Plant and Equipment
1.06	1.06.12	1.06.12.01	1.06.12.01.05	Gas Mains Supply
1.06	1.06.12	1.06.12.01	1.06.12.01.06	Telecommunications and Other Communication System Connections
1.06	1.06.12	1.06.12.01	1.06.12.01.07	External Fuel Storage and Piped Distribution Systems
1.06	1.06.12	1.06.12.01	1.06.12.01.08	External Security Systems
1.06	1.06.12	1.06.12.01	1.06.12.01.09	External / Street Lighting Systems
1.06	1.06.12	1.06.12.01	1.06.12.01.10	Local / District Heating Installations
1.06	1.06.12	1.06.12.01	1.06.12.01.11	Builder’s Work in Connection With External Services
1.06	1.06.13			**Prefabricated Buildings and Building Units**
1.06	1.06.13	1.06.13.01		**Prefabricated Buildings and Building Units and Minor Ancillary Buildings**
1.06	1.06.13	1.06.13.01	1.06.13.01.01	Complete Buildings
1.06	1.06.13	1.06.13.01	1.06.13.01.02	Building Units
1.06	1.06.13	1.06.13.01	1.06.13.01.03	Pods
1.06	1.06.13	1.06.13.01	1.06.13.01.04	Bike Stores
1.06	1.06.14			**Works to Existing Buildings**
1.06	1.06.14	1.06.14.01		**Minor Demolition Works and Alteration Works**
1.06	1.06.14	1.06.14.01	1.06.14.01.01	Minor Demolition Works and Alteration Works
1.06	1.06.14	1.06.14.02		**Repairs to Existing Services**
1.06	1.06.14	1.06.14.02	1.06.14.02.01	Repairs to Existing Services
1.06	1.06.14	1.06.14.03		**Damp Proof Courses / Fungus and Beetle Eradication**
1.06	1.06.14	1.06.14.03	1.06.14.03.01	Damp-proof Course / Fungus and Beetle Eradication
1.06	1.06.14	1.06.14.04		**Façade Retention**
1.06	1.06.14	1.06.14.04	1.06.14.04.01	Façade Retention
1.06	1.06.14	1.06.14.05		**Cleaning Existing Surfaces**
1.06	1.06.14	1.06.14.05	1.06.14.05.01	Cleaning Existing Surfaces
1.06	1.06.14	1.06.14.05	1.06.14.05.02	Protective Coatings to Existing Surfaces
1.06	1.06.14	1.06.14.06		**Renovation Works**
1.06	1.06.14	1.06.14.06	1.06.14.06.01	Masonry Repairs
1.06	1.06.14	1.06.14.06	1.06.14.06.02	Concrete Repairs
1.06	1.06.14	1.06.14.06	1.06.14.06.03	Metal Repairs
1.06	1.06.14	1.06.14.06	1.06.14.06.04	Timber Repairs
1.06	1.06.14	1.06.14.06	1.06.14.06.05	Plastics Repairs

Level 1	Level 2	Level 3	Level 4	Item
1.07				**Civil Engineering**
1.07	1.07.01			**Earthworks**
1.07	1.07.01	1.07.01.01		**Cuttings**
1.07	1.07.01	1.07.01.01	1.07.01.01.01	General excavation
1.07	1.07.01	1.07.01.01	1.07.01.01.02	Disposal
1.07	1.07.01	1.07.01.01	1.07.01.01.03	Filling
1.07	1.07.01	1.07.01.01	1.07.01.01.04	Filling Ancillaries
1.07	1.07.01	1.07.01.01	1.07.01.01.05	Grading to Profile
1.07	1.07.01	1.07.01.01	1.07.01.01.06	Landscaping
1.07	1.07.01	1.07.01.01	1.07.01.01.07	Ecology Works: state type
1.07	1.07.01	1.07.01.02		**Embankments**
1.07	1.07.01	1.07.01.02	1.07.01.02.01	General Excavation
1.07	1.07.01	1.07.01.02	1.07.01.02.02	Disposal
1.07	1.07.01	1.07.01.02	1.07.01.02.03	Filling
1.07	1.07.01	1.07.01.02	1.07.01.02.04	Filling Ancillaries
1.07	1.07.01	1.07.01.02	1.07.01.02.05	Grading to Profile
1.07	1.07.01	1.07.01.02	1.07.01.02.06	Landscaping
1.07	1.07.01	1.07.01.02	1.07.01.02.07	Ecology Works: state type
1.07	1.07.01	1.07.01.03		**Level Ground**
1.07	1.07.01	1.07.01.03	1.07.01.03.01	General Excavation
1.07	1.07.01	1.07.01.03	1.07.01.03.02	Disposal
1.07	1.07.01	1.07.01.03	1.07.01.03.03	Filling
1.07	1.07.01	1.07.01.03	1.07.01.03.04	Filling Ancillaries
1.07	1.07.01	1.07.01.03	1.07.01.03.05	Grading to Profile
1.07	1.07.01	1.07.01.03	1.07.01.03.06	Landscaping
1.07	1.07.01	1.07.01.03	1.07.01.03.07	Ecology Works: state type
1.07	1.07.01	1.07.01.04		**Preventative Earthworks**
1.07	1.07.01	1.07.01.04	1.07.01.04.01	Permanent Monitoring
1.07	1.07.01	1.07.01.04	1.07.01.04.02	Removing Overburden
1.07	1.07.01	1.07.01.04	1.07.01.04.03	Removing Vegetation and Scaling
1.07	1.07.01	1.07.01.04	1.07.01.04.04	Rock Bolting and Netting
1.07	1.07.01	1.07.01.04	1.07.01.04.05	Soil Nailing and Ground Anchors
1.07	1.07.01	1.07.01.04	1.07.01.04.06	Rock or Anti-vermin Netting
1.07	1.07.02			**Coastal and Estuarial Defences**
1.07	1.07.02	1.07.02.01		**Geotechnical and Specialist Processes**
1.07	1.07.02	1.07.02.01	1.07.02.01.01	Grouting
1.07	1.07.02	1.07.02.01	1.07.02.01.02	Diaphragm Walls
1.07	1.07.02	1.07.02.01	1.07.02.01.03	Ground Anchorages
1.07	1.07.02	1.07.02.02		**Protective Works**
1.07	1.07.02	1.07.02.02	1.07.02.02.01	Interlocking Sheet Piles
1.07	1.07.02	1.07.02.02	1.07.02.02.02	Rock Bolting and Netting
1.07	1.07.02	1.07.02.02	1.07.02.02.03	Soil Nailing and Ground Anchors
1.07	1.07.02	1.07.02.02	1.07.02.02.04	Rock or Anti-vermin Netting
1.07	1.07.02	1.07.02.03		**Groynes**
1.07	1.07.02	1.07.02.03	1.07.02.03.01	Rock Filling
1.07	1.07.02	1.07.02.03	1.07.02.03.02	Concrete
1.07	1.07.02	1.07.02.03	1.07.02.03.03	Timber
1.07	1.07.02	1.07.02.04		**Walls and Revetments**
1.07	1.07.02	1.07.02.04	1.07.02.04.01	Concrete Piles
1.07	1.07.02	1.07.02.04	1.07.02.04.02	Timber Piles
1.07	1.07.02	1.07.02.04	1.07.02.04.03	Masonry
1.07	1.07.02	1.07.02.04	1.07.02.04.04	Brickwork
1.07	1.07.02	1.07.02.04	1.07.02.04.05	Blockwork
1.07	1.07.02	1.07.02.04	1.07.02.04.06	Gabions
1.07	1.07.03			**Tunnels and Shafts**
1.07	1.07.03	1.07.03.01		**Excavation**
1.07	1.07.03	1.07.03.01	1.07.03.01.01	Tunnels: Bored
1.07	1.07.03	1.07.03.01	1.07.03.01.02	Tunnels: Cut and Cover
1.07	1.07.03	1.07.03.01	1.07.03.01.03	Adit
1.07	1.07.03	1.07.03.01	1.07.03.01.04	Shafts
1.07	1.07.03	1.07.03.01	1.07.03.01.05	Cavities

1.07	1.07.03	1.07.03.02		**Linings**
1.07	1.07.03	1.07.03.02	1.07.03.02.01	Masonry Lining
1.07	1.07.03	1.07.03.02	1.07.03.02.02	Segmental Lining
1.07	1.07.03	1.07.03.02	1.07.03.02.03	Applied Lining
1.07	1.07.03	1.07.03.02	1.07.03.02.04	Cut and Cover Tunnel Lining
1.07	1.07.03	1.07.03.03		**Support Stabilisation**
1.07	1.07.03	1.07.03.03	1.07.03.03.01	Natural Surfaces
1.07	1.07.03	1.07.03.03	1.07.03.03.02	Internal Support
1.07	1.07.03	1.07.03.03	1.07.03.03.03	Pressure Grouting
1.07	1.07.03	1.07.03.03	1.07.03.03.04	Forward Probing
1.07	1.07.03	1.07.03.04		**Portals**
1.07	1.07.03	1.07.03.04	1.07.03.04.01	Walls: state material
1.07	1.07.03	1.07.03.04	1.07.03.04.02	Surface Features
1.07	1.07.03	1.07.03.05		**Furniture**
1.07	1.07.03	1.07.03.05	1.07.03.05.01	Signs: state type
1.07	1.07.04			**Subways and Underpasses**
1.07	1.07.04	1.07.04.01		**Excavation**
1.07	1.07.04	1.07.04.01	1.07.04.01.01	Subway or Underpass
1.07	1.07.04	1.07.04.01	1.07.04.01.02	Footings
1.07	1.07.04	1.07.04.02		**Foundations**
1.07	1.07.04	1.07.04.02	1.07.04.02.01	Piled Foundations
1.07	1.07.04	1.07.04.02	1.07.04.02.02	Standard Foundations
1.07	1.07.04	1.07.04.02	1.07.04.02.03	Underpinning
1.07	1.07.04	1.07.04.03		**Retaining Wall**
1.07	1.07.04	1.07.04.03	1.07.04.03.01	In-situ Construction
1.07	1.07.04	1.07.04.03	1.07.04.03.02	Pre-fabricated Units
1.07	1.07.04	1.07.04.03	1.07.04.03.03	Piled and Faced
1.07	1.07.04	1.07.04.04		**Slabs**
1.07	1.07.04	1.07.04.04	1.07.04.04.01	Floors
1.07	1.07.04	1.07.04.04	1.07.04.04.02	Roofs
1.07	1.07.04	1.07.04.05		**Ramps, Staircases and Landings**
1.07	1.07.04	1.07.04.05	1.07.04.05.01	Staircases
1.07	1.07.04	1.07.04.05	1.07.04.05.02	Landings and Half Landings
1.07	1.07.04	1.07.04.05	1.07.04.05.03	Ramps
1.07	1.07.04	1.07.04.05	1.07.04.05.04	Balustrading / Handrailing: state size and type
1.07	1.07.04	1.07.04.05	1.07.04.05.05	Access Ladders: state size and type
1.07	1.07.04	1.07.04.06		**Finishes and Furniture**
1.07	1.07.04	1.07.04.06	1.07.04.06.01	Floor
1.07	1.07.04	1.07.04.06	1.07.04.06.02	Walls
1.07	1.07.04	1.07.04.06	1.07.04.06.03	Soffit
1.07	1.07.04	1.07.04.06	1.07.04.06.04	Signs
1.07	1.07.04	1.07.04.06	1.07.04.06.05	Lighting
1.07	1.07.05			**Bridges and Viaducts for Road or Rail Vehicles**
1.07	1.07.05	1.07.05.01		**Foundations**
1.07	1.07.05	1.07.05.01	1.07.05.01.01	Piles / Caisson
1.07	1.07.05	1.07.05.01	1.07.05.01.02	Concrete Footings
1.07	1.07.05	1.07.05.02		**Support Structures**
1.07	1.07.05	1.07.05.02	1.07.05.02.01	Pier
1.07	1.07.05	1.07.05.02	1.07.05.02.02	Abutment
1.07	1.07.05	1.07.05.02	1.07.05.02.03	Wing Walls
1.07	1.07.05	1.07.05.02	1.07.05.02.04	Surface finishes
1.07	1.07.05	1.07.05.02	1.07.05.02.05	Cill Beams
1.07	1.07.05	1.07.05.02	1.07.05.02.06	Bridge Bearings
1.07	1.07.05	1.07.05.03		**Deck**
1.07	1.07.05	1.07.05.03	1.07.05.03.01	Beams
1.07	1.07.05	1.07.05.03	1.07.05.03.02	Structural Decking
1.07	1.07.05	1.07.05.03	1.07.05.03.03	Way Beam / Longitudinal Timber
1.07	1.07.05	1.07.05.03	1.07.05.03.04	Cable Ducts
1.07	1.07.05	1.07.05.04		**Walkways and Landings**
1.07	1.07.05	1.07.05.04	1.07.05.04.01	Flooring
1.07	1.07.05	1.07.05.04	1.07.05.04.02	Ramps
1.07	1.07.05	1.07.05.04	1.07.05.04.03	Staircases

1.07	1.07.05	1.07.05.05		**Pavings and Surfacing**
1.07	1.07.05	1.07.05.05	1.07.05.05.01	Surfacing
1.07	1.07.05	1.07.05.05	1.07.05.05.02	Road Marking
1.07	1.07.05	1.07.05.05	1.07.05.05.03	Kerbs and Channels
1.07	1.07.05	1.07.05.05	1.07.05.05.04	Waterproofing
1.07	1.07.05	1.07.05.06		**Parapets**
1.07	1.07.05	1.07.05.06	1.07.05.06.01	Normal Containment Parapet
1.07	1.07.05	1.07.05.06	1.07.05.06.02	High Containment Parapet
1.07	1.07.05	1.07.05.06	1.07.05.06.03	Very High Containment Parapet
1.07	1.07.05	1.07.05.06	1.07.05.06.04	Ornamental / Listed Parapet
1.07	1.07.05	1.07.05.06	1.07.05.06.05	Balustrade
1.07	1.07.05	1.07.05.06	1.07.05.06.06	Parapet Handrails
1.07	1.07.05	1.07.05.06	1.07.05.06.07	Anti-trespass Wall / Roof
1.07	1.07.05	1.07.05.06	1.07.05.06.08	Suicide Cage
1.07	1.07.05	1.07.05.07		**Furniture**
1.07	1.07.05	1.07.05.07	1.07.05.07.01	Signs
1.07	1.07.05	1.07.05.08		**Drainage to Structures**
1.07	1.07.05	1.07.05.08	1.07.05.08.01	Pipe Work
1.07	1.07.05	1.07.05.08	1.07.05.08.02	Gullies with Gratings
1.07	1.07.05	1.07.05.08	1.07.05.08.03	Manholes and Inspection Chambers: state type
1.07	1.07.05	1.07.05.09		**Approaches**
1.07	1.07.05	1.07.05.09	1.07.05.09.01	Excavation and Disposal
1.07	1.07.05	1.07.05.09	1.07.05.09.02	Filling to Structures
1.07	1.07.05	1.07.05.09	1.07.05.09.03	Surfacing
1.07	1.07.05	1.07.05.09	1.07.05.09.04	Kerbs, Channels and Edgings
1.07	1.07.06			**Footbridges**
1.07	1.07.06	1.07.06.01		**Foundations**
1.07	1.07.06	1.07.06.01	1.07.06.01.01	Piles / Caisson
1.07	1.07.06	1.07.06.01	1.07.06.01.02	Concrete Footings
1.07	1.07.06	1.07.06.02		**Abutments and Piers**
1.07	1.07.06	1.07.06.02	1.07.06.02.01	Pier
1.07	1.07.06	1.07.06.02	1.07.06.02.02	Abutment
1.07	1.07.06	1.07.06.02	1.07.06.02.03	Wing Walls
1.07	1.07.06	1.07.06.02	1.07.06.02.04	Surface Finishes
1.07	1.07.06	1.07.06.02	1.07.06.02.05	Cill Beams
1.07	1.07.06	1.07.06.02	1.07.06.02.06	Bridge Bearings
1.07	1.07.06	1.07.06.03		**Deck**
1.07	1.07.06	1.07.06.03	1.07.06.03.01	Beams
1.07	1.07.06	1.07.06.03	1.07.06.03.02	Structural Decking
1.07	1.07.06	1.07.06.03	1.07.06.03.03	Way Beam / Longitudinal Timber
1.07	1.07.06	1.07.06.03	1.07.06.03.04	Cable Ducts
1.07	1.07.06	1.07.06.04		**Walkways and Landings**
1.07	1.07.06	1.07.06.04	1.07.06.04.01	Flooring
1.07	1.07.06	1.07.06.04	1.07.06.04.02	Ramps
1.07	1.07.06	1.07.06.04	1.07.06.04.03	Staircases
1.07	1.07.06	1.07.06.05		**Pavings and Surfacing**
1.07	1.07.06	1.07.06.05	1.07.06.05.01	Surfacing
1.07	1.07.06	1.07.06.05	1.07.06.05.02	Road Marking
1.07	1.07.06	1.07.06.05	1.07.06.05.03	Kerbs and Channels
1.07	1.07.06	1.07.06.05	1.07.06.05.04	Waterproofing
1.07	1.07.06	1.07.06.06		**Parapets**
1.07	1.07.06	1.07.06.06	1.07.06.06.01	Normal Containment Parapet
1.07	1.07.06	1.07.06.06	1.07.06.06.02	High Containment Parapet
1.07	1.07.06	1.07.06.06	1.07.06.06.03	Very High Containment Parapet
1.07	1.07.06	1.07.06.06	1.07.06.06.04	Ornamental / Listed Parapet
1.07	1.07.06	1.07.06.06	1.07.06.06.05	Balustrade
1.07	1.07.06	1.07.06.06	1.07.06.06.06	Parapet Handrails
1.07	1.07.06	1.07.06.06	1.07.06.06.07	Anti-trespass Wall / Roof
1.07	1.07.06	1.07.06.06	1.07.06.06.08	Suicide Cage
1.07	1.07.06	1.07.06.07		**Furniture**
1.07	1.07.06	1.07.06.07	1.07.06.07.01	Signs
1.07	1.07.06	1.07.06.08		**Drainage to Structures**

1.07	1.07.06	1.07.06.08	1.07.06.08.01	Pipe Work
1.07	1.07.06	1.07.06.08	1.07.06.08.02	Gullies with Gratings
1.07	1.07.06	1.07.06.08	1.07.06.08.03	Manholes and Inspection Chambers: state type
1.07	1.07.06	1.07.06.09		**Approaches**
1.07	1.07.06	1.07.06.09	1.07.06.09.01	Excavation and Disposal
1.07	1.07.06	1.07.06.09	1.07.06.09.02	Filling to Structures
1.07	1.07.06	1.07.06.09	1.07.06.09.03	Surfacing
1.07	1.07.06	1.07.06.09	1.07.06.09.04	Kerbs, Channels and Edgings
1.07	1.07.07			**Platforms**
1.07	1.07.07	1.07.07.01		**Foundations**
1.07	1.07.07	1.07.07.01	1.07.07.01.01	Piles
1.07	1.07.07	1.07.07.01	1.07.07.01.02	Concrete Footings
1.07	1.07.07	1.07.07.01	1.07.07.01.03	Support Structure to Platforms
1.07	1.07.07	1.07.07.02		**Deck and Supporting Structure**
1.07	1.07.07	1.07.07.02	1.07.07.02.01	Support Structure to Platforms: state type
1.07	1.07.07	1.07.07.02	1.07.07.02.02	Structural Decking : state type
1.07	1.07.07	1.07.07.03		**Access Structures for Platforms**
1.07	1.07.07	1.07.07.03	1.07.07.03.01	Ramps
1.07	1.07.07	1.07.07.03	1.07.07.03.02	Staircases
1.07	1.07.07	1.07.07.03	1.07.07.03.03	Access Arrangements (Ladders) to Roof / Canopies
1.07	1.07.07	1.07.07.03	1.07.07.03.04	Balustrading / Handrails
1.07	1.07.07	1.07.07.04		**Paving and Surfacing**
1.07	1.07.07	1.07.07.04	1.07.07.04.01	Platform Copings
1.07	1.07.07	1.07.07.04	1.07.07.04.02	Tactile Paving
1.07	1.07.07	1.07.07.04	1.07.07.04.03	Surfacing / Finishes to Platforms: state type
1.07	1.07.07	1.07.07.04	1.07.07.04.04	Platform Markings
1.07	1.07.07	1.07.07.05		**Roof and Canopy Structure and Coverings**
1.07	1.07.07	1.07.07.05	1.07.07.05.01	Support Structure to Roof / Canopy: state type
1.07	1.07.07	1.07.07.05	1.07.07.05.02	Coverings
1.07	1.07.07	1.07.07.06		**Platform Fittings and Furniture**
1.07	1.07.07	1.07.07.06	1.07.07.06.01	Signs / Notices
1.07	1.07.07	1.07.07.06	1.07.07.06.02	Seating
1.07	1.07.07	1.07.07.07		**Drainage and Ducts**
1.07	1.07.07	1.07.07.07	1.07.07.07.01	Pipework Above Ground: state type and size
1.07	1.07.07	1.07.07.07	1.07.07.07.02	Pipework Below Ground: state type and size
1.07	1.07.07	1.07.07.07	1.07.07.07.03	Cable Ducts
1.07	1.07.07	1.07.07.07	1.07.07.07.04	Manholes, Catchpits, Turning Chambers and other Inspection Pits: state type and size
1.07	1.07.08			**Retaining Walls**
1.07	1.07.08	1.07.08.01		**Foundations**
1.07	1.07.08	1.07.08.01	1.07.08.01.01	Foundations: Linear
1.07	1.07.08	1.07.08.01	1.07.08.01.02	Foundations: Isolated
1.07	1.07.08	1.07.08.01	1.07.08.01.03	Piling
1.07	1.07.08	1.07.08.01	1.07.08.01.04	Filling
1.07	1.07.08	1.07.08.02		**Retaining Walls**
1.07	1.07.08	1.07.08.02	1.07.08.02.01	Walls: Gravity Type
1.07	1.07.08	1.07.08.02	1.07.08.02.02	Walls: Cantilever
1.07	1.07.08	1.07.08.02	1.07.08.02.03	Walls: King Post Construction
1.07	1.07.08	1.07.08.02	1.07.08.02.04	Walls: Piled Construction
1.07	1.07.08	1.07.08.02	1.07.08.02.05	Surface Feature
1.07	1.07.08	1.07.08.02	1.07.08.02.06	Interlocking Sheet Piles
1.07	1.07.08	1.07.08.02	1.07.08.02.07	Waterproof Membranes
1.07	1.07.08	1.07.08.02	1.07.08.02.08	Gabions
1.07	1.07.08	1.07.08.02	1.07.08.02.09	Drain Hole or Weep Hole
1.07	1.07.09			**Fencing and Enclosures**
1.07	1.07.09	1.07.09.01		**Fencing and Railings**
1.07	1.07.09	1.07.09.01	1.07.09.01.01	Fences: state type
1.07	1.07.09	1.07.09.01	1.07.09.01.02	Gates: Personnel
1.07	1.07.09	1.07.09.01	1.07.09.01.03	Gates: Vehicular
1.07	1.07.09	1.07.09.01	1.07.09.01.04	Stiles: state type
1.07	1.07.09	1.07.09.01	1.07.09.01.05	Avalanche Fencing
1.07	1.07.09	1.07.09.01	1.07.09.01.06	Catch Walls: state type
1.07	1.07.09	1.07.09.01	1.07.09.01.07	Take Down and Dispose of Fencing: state size and type

1.07	1.07.09	1.07.09.01	1.07.09.01.08	Take Down and Dispose of Gates and Stiles: state size and type
1.07	1.07.09	1.07.09.02		**Barriers and Guard Rails**
1.07	1.07.09	1.07.09.02	1.07.09.02.01	Fixed Barriers
1.07	1.07.09	1.07.09.02	1.07.09.02.02	Access Barriers: Personnel
1.07	1.07.09	1.07.09.02	1.07.09.02.03	Access Barriers: Vehicular
1.07	1.07.09	1.07.09.02	1.07.09.02.04	Take Down and Dispose of Vehicular Barriers: state type
1.07	1.07.09	1.07.09.02	1.07.09.02.05	Take Down and Dispose of Pedestrian Guard Rails : state type
1.07	1.07.10			**General Drainage**
1.07	1.07.10	1.07.10.01		**Surface Water Drainage**
1.07	1.07.10	1.07.10.01	1.07.10.01.01	Drain Pipes and Trenches: state size and depth
1.07	1.07.10	1.07.10.01	1.07.10.01.02	Channels and Gratings
1.07	1.07.10	1.07.10.01	1.07.10.01.03	Gullies
1.07	1.07.10	1.07.10.01	1.07.10.01.04	Manholes and Inspection Chambers: state type
1.07	1.07.10	1.07.10.01	1.07.10.01.05	Interceptors
1.07	1.07.10	1.07.10.01	1.07.10.01.06	Connections to Public Mains Drainage
1.07	1.07.10	1.07.10.02		**Foul Water Drainage**
1.07	1.07.10	1.07.10.02	1.07.10.02.01	Drain Pipes and Trenches: state size and depth
1.07	1.07.10	1.07.10.02	1.07.10.02.02	Channels and Gratings
1.07	1.07.10	1.07.10.02	1.07.10.02.03	Gullies
1.07	1.07.10	1.07.10.02	1.07.10.02.04	Manholes and Inspection Chambers: state type
1.07	1.07.10	1.07.10.02	1.07.10.02.05	Connections to Public Mains Drainage
1.07	1.07.10	1.07.10.03		**External Chemical, Toxic and Industrial Liquid Waste Drainage**
1.07	1.07.10	1.07.10.03	1.07.10.03.01	Drain Pipes and Trenches: state size and depth
1.07	1.07.10	1.07.10.03	1.07.10.03.02	Drain Pipes and Supports Above Ground: state size and support type / spacings
1.07	1.07.10	1.07.10.03	1.07.10.03.03	Channels and Gratings: state type and size
1.07	1.07.10	1.07.10.03	1.07.10.03.04	Manholes and Inspection Chambers: state size and type
1.07	1.07.10	1.07.10.03	1.07.10.03.05	Storage Tanks: state type and size
1.07	1.07.10	1.07.10.04		**Balancing Ponds and Retention Basins**
1.07	1.07.10	1.07.10.04	1.07.10.04.01	Ponds: Excavation and Disposal
1.07	1.07.10	1.07.10.04	1.07.10.04.02	Watercourses: Excavation and Disposal
1.07	1.07.10	1.07.10.04	1.07.10.04.03	Linings: Balancing Ponds
1.07	1.07.10	1.07.10.04	1.07.10.04.04	Linings: Watercourses
1.07	1.07.10	1.07.10.05		**French Drains, Rubble Drains, Ditches and Trenches**
1.07	1.07.10	1.07.10.05	1.07.10.05.01	French Drains: state pipes and filling
1.07	1.07.10	1.07.10.05	1.07.10.05.02	Lined Ditches
1.07	1.07.10	1.07.10.05	1.07.10.05.03	Soakaways
1.07	1.07.10	1.07.10.05	1.07.10.05.04	Outfalls Including Fittings
1.07	1.07.10	1.07.10.06		**Culverts**
1.07	1.07.10	1.07.10.06	1.07.10.06.01	New Culverts: state type
1.07	1.07.10	1.07.10.06	1.07.10.06.02	Existing Culverts: Lining
1.07	1.07.10	1.07.10.07		**Testing and Commissioning**
1.07	1.07.10	1.07.10.07	1.07.10.07.01	Testing: During the Progress of the Works
1.07	1.07.10	1.07.10.07	1.07.10.07.02	Testing : On Completion of the Works
1.07	1.07.10	1.07.10.07	1.07.10.07.03	Commissioning: Work Completed in Sections
1.07	1.07.10	1.07.10.07	1.07.10.07.04	Commissioning: Co-Ordination of Sectional Work
1.07	1.07.10	1.07.10.07	1.07.10.07.05	Commissioning and Handover
1.07	1.07.10	1.07.10.08		**Abandonment and Recovery of Drainage**
1.07	1.07.10	1.07.10.08	1.07.10.08.01	Excavation and Disposal of Buried Pipe Drainage: state type and depth
1.07	1.07.10	1.07.10.08	1.07.10.08.02	Take Up and Dispose Culverts: state type and size
1.07	1.07.10	1.07.10.08	1.07.10.08.03	Remove Manholes and Inspection Chambers: state size and type
1.07	1.07.10	1.07.10.08	1.07.10.08.04	Take Up and Dispose of Gullies and Fill Void
1.07	1.07.11			**Track Foundations**
1.07	1.07.11	1.07.11.01		**Ballasted Track Bed**
1.07	1.07.11	1.07.11.01	1.07.11.01.01	Excavation and Disposal
1.07	1.07.11	1.07.11.01	1.07.11.01.02	Filling to Structures
1.07	1.07.11	1.07.11.01	1.07.11.01.03	Blanket and Geotextile Layer
1.07	1.07.11	1.07.11.01	1.07.11.01.04	Excavation and Disposal of Track Foundation Materials : state type
1.07	1.07.11	1.07.11.02		**Concrete Paved Track Bed**
1.07	1.07.11	1.07.11.02	1.07.11.02.01	Excavation and Disposal
1.07	1.07.11	1.07.11.02	1.07.11.02.02	Filling to Structures
1.07	1.07.11	1.07.11.02	1.07.11.02.03	Blanket and Geotextile Layer
1.07	1.07.11	1.07.11.02	1.07.11.02.04	Excavation and Disposal of Track Foundation Materials : state type

1.07	1.07.12			**Roads, Pavements and Hardstanding's**
1.07	1.07.12	1.07.12.01		**Roads**
1.07	1.07.12	1.07.12.01	1.07.12.01.01	Excavation and Disposal
1.07	1.07.12	1.07.12.01	1.07.12.01.02	Filling to Structures
1.07	1.07.12	1.07.12.01	1.07.12.01.03	Surfaced Access Ways: Vehicular
1.07	1.07.12	1.07.12.01	1.07.12.01.04	Surfaced Access Ways: Pedestrian
1.07	1.07.12	1.07.12.01	1.07.12.01.05	Surfacing to Ducting or Troughing: Paved Finish
1.07	1.07.12	1.07.12.01	1.07.12.01.06	Kerbs, Channels and Edgings
1.07	1.07.12	1.07.12.02		**Hardstanding's and Carparks**
1.07	1.07.12	1.07.12.02	1.07.12.02.01	Excavation and Disposal
1.07	1.07.12	1.07.12.02	1.07.12.02.02	Filling to Structures
1.07	1.07.12	1.07.12.02	1.07.12.02.03	Surfaced Access Ways: Vehicular
1.07	1.07.12	1.07.12.02	1.07.12.02.04	Surfaced Access Ways: Pedestrian
1.07	1.07.12	1.07.12.02	1.07.12.02.05	Surfacing to Ducting or Troughing: Paved Finish
1.07	1.07.12	1.07.12.02	1.07.12.02.06	Kerbs, Channels and Edgings
1.07	1.07.12	1.07.12.03		**Pavements and Walkways**
1.07	1.07.12	1.07.12.03	1.07.12.03.01	Excavation and Disposal
1.07	1.07.12	1.07.12.03	1.07.12.03.02	Filling to Structures
1.07	1.07.12	1.07.12.03	1.07.12.03.03	Surfaced Access Ways: Vehicular
1.07	1.07.12	1.07.12.03	1.07.12.03.04	Surfaced Access Ways: Pedestrian
1.07	1.07.12	1.07.12.03	1.07.12.03.05	Surfacing to Ducting or Troughing: Paved Finish
1.07	1.07.12	1.07.12.03	1.07.12.03.06	Kerbs, Channels and Edgings
1.07	1.07.12	1.07.12.04		**Track Asset Walkways**
1.07	1.07.12	1.07.12.04	1.07.12.04.01	Excavation and Disposal
1.07	1.07.12	1.07.12.04	1.07.12.04.02	Filling to Structures
1.07	1.07.12	1.07.12.04	1.07.12.04.03	Surfaced Access Ways: Vehicular
1.07	1.07.12	1.07.12.04	1.07.12.04.04	Surfaced Access Ways: Pedestrian
1.07	1.07.12	1.07.12.04	1.07.12.04.05	Surfacing to Ducting or Troughing: Paved Finish
1.07	1.07.12	1.07.12.04	1.07.12.04.06	Kerbs, Channels and Edgings
1.07	1.07.12	1.07.12.05		**Service Ducts Within Hardstanding's**
1.07	1.07.12	1.07.12.05	1.07.12.05.01	Cable Routes: state type
1.07	1.07.12	1.07.12.05	1.07.12.05.02	Service Ducts: state details
1.07	1.07.12	1.07.12.06		**[Not used]**
1.07	1.07.12	1.07.12.07		**Other Street Furniture**
1.07	1.07.12	1.07.12.07	1.07.12.07.01	Site / Street Furniture: state type
1.07	1.07.12	1.07.12.07	1.07.12.07.02	Ornamental Features: state type
1.07	1.07.12	1.07.12.08		**Abandonment and Recovery of Roads, Pavings and Hardstanding's**
1.07	1.07.12	1.07.12.08	1.07.12.08.01	Break Up and Dispose of Surfacing and Paving
1.07	1.07.12	1.07.12.08	1.07.12.08.02	Take Up and Dispose of Kerbs, Edgings and Associated Concrete Backing: state type
1.07	1.07.12	1.07.12.08	1.07.12.08.03	Take Up and Recover Lighting Cable Routes and Ducts: state type and size
1.07	1.07.12	1.07.12.08	1.07.12.08.04	Take Up and Recover Light Fittings : state type and size
1.07	1.07.12	1.07.12.08	1.07.12.08.05	Take Up and Recover Other Street Furniture: state type and size
1.07	1.07.13			**Landscaping and Ecology Outside Railway Corridor**
1.07	1.07.13	1.07.13.01		**Soft Landscaping, Planting and Irrigation Systems**
1.07	1.07.13	1.07.13.01	1.07.13.01.01	Seeding and Turfing
1.07	1.07.13	1.07.13.01	1.07.13.01.02	External Planting: state type
1.07	1.07.13	1.07.13.01	1.07.13.01.03	Irrigation Systems: state type
1.07	1.07.13	1.07.13.02		**Ecology Works**
1.07	1.07.13	1.07.13.02	1.07.13.02.01	Ecology Works: state type
1.07	1.07.14			**Troughing**
1.07	1.07.14	1.07.14.01		**Troughing - Ground Level**
1.07	1.07.14	1.07.14.01	1.07.14.01.01	Traditional Concrete Troughing
1.07	1.07.14	1.07.14.01	1.07.14.01.02	Concrete Based Troughing
1.07	1.07.14	1.07.14.01	1.07.14.01.03	Non-cementitious Troughing
1.07	1.07.14	1.07.14.01	1.07.14.01.04	Transition Unit
1.07	1.07.14	1.07.14.01	1.07.14.01.05	T' Piece
1.07	1.07.14	1.07.14.01	1.07.14.01.06	De-lid and Lid Existing Troughing to Receive Cables
1.07	1.07.14	1.07.14.01	1.07.14.01.07	Abandonment and Recovery of Containment and Trough Route: state type
1.07	1.07.14	1.07.14.02		**Troughing - Ground Level Partly Buried**
1.07	1.07.14	1.07.14.02	1.07.14.02.01	Traditional Concrete Troughing
1.07	1.07.14	1.07.14.02	1.07.14.02.02	Concrete Based Troughing
1.07	1.07.14	1.07.14.02	1.07.14.02.03	Non-cementitious Troughing

1.07	1.07.14	1.07.14.02	1.07.14.02.04	Transition Unit
1.07	1.07.14	1.07.14.02	1.07.14.02.05	T' Piece
1.07	1.07.14	1.07.14.02	1.07.14.02.06	De-lid and Lid Existing Troughing to Receive Cables
1.07	1.07.14	1.07.14.02	1.07.14.02.07	Abandonment and Recovery of Containment and Trough Route: state type
1.07	1.07.14	1.07.14.03		**Troughing - Elevated**
1.07	1.07.14	1.07.14.03	1.07.14.03.01	Traditional Concrete Troughing
1.07	1.07.14	1.07.14.03	1.07.14.03.02	Concrete Based Troughing
1.07	1.07.14	1.07.14.03	1.07.14.03.03	Non-cementitious Troughing
1.07	1.07.14	1.07.14.03	1.07.14.03.04	Transition Unit
1.07	1.07.14	1.07.14.03	1.07.14.03.05	T' Piece
1.07	1.07.14	1.07.14.03	1.07.14.03.06	De-lid and Lid Existing Troughing to Receive Cables
1.07	1.07.14	1.07.14.03	1.07.14.03.07	Abandonment and Recovery of Containment and Trough Route: state type
1.07	1.07.15			**Crossings and Duct Ways**
1.07	1.07.15	1.07.15.01		**Buried Duct Ways: General**
1.07	1.07.15	1.07.15.01	1.07.15.01.01	Ducts: state type
1.07	1.07.15	1.07.15.01	1.07.15.01.02	Draw pits and Chambers: state type
1.07	1.07.15	1.07.15.01	1.07.15.01.03	Cable Bridge: state type
1.07	1.07.15	1.07.15.02		**Under Track Crossings**
1.07	1.07.15	1.07.15.02	1.07.15.02.01	Ducts: state type
1.07	1.07.15	1.07.15.02	1.07.15.02.02	Draw pits and Chambers: state type
1.07	1.07.15	1.07.15.02	1.07.15.02.03	Cable Bridge: state type
1.07	1.07.15	1.07.15.03		**Under Rail Crossings**
1.07	1.07.15	1.07.15.03	1.07.15.03.01	Ducts: state type
1.07	1.07.15	1.07.15.03	1.07.15.03.02	Draw pits and Chambers: state type
1.07	1.07.15	1.07.15.03	1.07.15.03.03	Cable Bridge: state type
1.07	1.07.15	1.07.15.04		**Under Road Crossings**
1.07	1.07.15	1.07.15.04	1.07.15.04.01	Ducts: state type
1.07	1.07.15	1.07.15.04	1.07.15.04.02	Draw pits and Chambers: state type
1.07	1.07.15	1.07.15.04	1.07.15.04.03	Cable Bridge: state type
1.07	1.07.15	1.07.15.05		**Over Track Crossings**
1.07	1.07.15	1.07.15.05	1.07.15.05.01	Ducts: state type
1.07	1.07.15	1.07.15.05	1.07.15.05.02	Draw pits and Chambers: state type
1.07	1.07.15	1.07.15.05	1.07.15.05.03	Cable Bridge: state type

Level 1	Level 2	Level 3	Level 4	Item
1.08				**Enabling Works**
1.08	1.08.01			**Extra Ordinary Site Investigation Works**
1.08	1.08.01	1.08.01.01		**Archaeological Investigations**
1.08	1.08.01	1.08.01	1.08.01.01.01	Physical Archaeological Investigation
1.08	1.08.01	1.08.01	1.08.01.01.02	Attendance on Archaeologist
1.08	1.08.01	1.08.01.02		**Reptile / Wildlife Investigation**
1.08	1.08.01	1.08.01.02	1.08.01.02.01	Trapping and Relocation of Species
1.08	1.08.01	1.08.01.02	1.08.01.02.02	Temporary Fences and/or Barriers
1.08	1.08.01	1.08.01.03		**Other Extraordinary Site Investigation Works**
1.08	1.08.01	1.08.01.03	1.08.01.03.01	Unexploded Munitions or Other
1.08	1.08.01	1.08.01.03	1.08.01.03.02	Ordnance Other Investigations: State Component Cost Item
1.08	1.08.02			**Site Clearance and Preparation Works**
1.08	1.08.02	1.08.02.01		**Site Clearance**
1.08	1.08.02	1.08.02.01	1.08.02.01.01	General Clearance
1.08	1.08.02	1.08.02.01	1.08.02.01.02	Clearance of Vegetation
1.08	1.08.02	1.08.02.01	1.08.02.01.03	Surveys
1.08	1.08.02	1.08.02.01	1.08.02.01.04	Management of Shrubs, Bushes and Trees
1.08	1.08.02	1.08.02.02		**Toxic / Hazardous Materials**
1.08	1.08.02	1.08.02.02	1.08.02.02.01	Toxic and / or Hazardous Parts of Building Fabric
1.08	1.08.02	1.08.02.02	1.08.02.02.02	Toxic and / or Hazardous Components from Service Installations
1.08	1.08.02	1.08.02.03		**Contaminated Land**
1.08	1.08.02	1.08.02.03	1.08.02.03.01	Contaminated Ground: Removal
1.08	1.08.02	1.08.02.03	1.08.02.03.02	Contaminated Ground: Treatment
1.08	1.08.02	1.08.02.04		**Eradication of Plant Growth**
1.08	1.08.02	1.08.02.04	1.08.02.04.01	Invasive Plant Growth: Removal
1.08	1.08.02	1.08.02.04	1.08.02.04.02	Invasive Plant Growth: Treatment
1.08	1.08.02	1.08.02.05		**Specialist Ground Works**
1.08	1.08.02	1.08.02.05	1.08.02.05.01	Site De-watering and Pumping
1.08	1.08.02	1.08.02.05	1.08.02.05.02	Soil Stabilisation
1.08	1.08.02	1.08.02.05	1.08.02.05.03	Ground Gas Ventilation
1.08	1.08.02	1.08.02.05	1.08.02.05.04	Compaction
1.08	1.08.02	1.08.02.05	1.08.02.05.05	Compensation Grouting
1.08	1.08.02	1.08.02.06		**Utility Diversion Works**
1.08	1.08.02	1.08.02.06	1.08.02.06.01	Diversions and Interruptions
1.08	1.08.02	1.08.02.06	1.08.02.06.02	Hardstanding's
1.08	1.08.02	1.08.02.06	1.08.02.06.03	Bridges and Walkways
1.08	1.08.03			**Structure Specific Enabling Works**
1.08	1.08.03	1.08.03.01		**Demolition Works**
1.08	1.08.03	1.08.03.01	1.08.03.01.01	Demolition: Entire Structures
1.08	1.08.03	1.08.03.01	1.08.03.01.02	Demolition: Partial Structures
1.08	1.08.03	1.08.03.01	1.08.03.01.03	Retention of Structures
1.08	1.08.03	1.08.03.02		**Permanent Alterations**
1.08	1.08.03	1.08.03.02	1.08.03.02.01	Underbridges
1.08	1.08.03	1.08.03.02	1.08.03.02.02	Overbridges
1.08	1.08.03	1.08.03.02	1.08.03.02.03	Tunnels
1.08	1.08.03	1.08.03.02	1.08.03.02.04	Platforms
1.08	1.08.03	1.08.03.02	1.08.03.02.05	Cables and Containment
1.08	1.08.03	1.08.03.03		**Temporary Alterations**
1.08	1.08.03	1.08.03.03	1.08.03.03.01	Permanent Way: Removal and Reinstatement
1.08	1.08.03	1.08.03.03	1.08.03.03.02	Railway Control System Equipment Removal and Reinstatement
1.08	1.08.03	1.08.03.03	1.08.03.03.03	Level Crossings
1.08	1.08.03	1.08.03.03	1.08.03.03.04	Overhead Line Equipment (OLE) Systems: Removal and Reinstatement
1.08	1.08.03	1.08.03.03	1.08.03.03.05	Telecommunication Equipment: Removal and Reinstatement
1.08	1.08.03	1.08.03.03	1.08.03.03.06	Platform and Building Furniture and Equipment: Removal and Reinstatement
1.08	1.08.03	1.08.03.03	1.08.03.03.07	Cables and Containment: Removal and Reinstatement
1.08	1.08.03	1.08.03.03	1.08.03.03.08	Boundary Fencing and Enclosures: Removal and Reinstatement

Level 1	Level 2	Level 3	Level 4	Item
1.09				**Rolling Stock**
1.09	1.09.01			**Passenger Rolling Stock**
1.09	1.09.01	1.09.01.01		**Driving Car**
1.09	1.09.01	1.09.01.01	1.09.01.01.01	Shell: including Painting
1.09	1.09.01	1.09.01.01	1.09.01.01.02	Interior Fit Out and Finishes: including Doors
1.09	1.09.01	1.09.01.01	1.09.01.01.03	Glazing / Windows
1.09	1.09.01	1.09.01.01	1.09.01.01.04	Bogies
1.09	1.09.01	1.09.01.01	1.09.01.01.05	Braking
1.09	1.09.01	1.09.01.01	1.09.01.01.06	Articulation
1.09	1.09.01	1.09.01.01	1.09.01.01.07	Traction Motors
1.09	1.09.01	1.09.01.01	1.09.01.01.08	Coupling
1.09	1.09.01	1.09.01.01	1.09.01.01.09	Control and Communications
1.09	1.09.01	1.09.01.01	1.09.01.01.10	Auxiliary Equipment and Batteries
1.09	1.09.01	1.09.01.01	1.09.01.01.11	Heating, Ventilation and Air Conditioning
1.09	1.09.01	1.09.01.01	1.09.01.01.12	Driver's Console and Cab Equipment
1.09	1.09.01	1.09.01.02		**Motor Car**
1.09	1.09.01	1.09.01.02	1.09.01.02.01	Shell: including Painting
1.09	1.09.01	1.09.01.02	1.09.01.02.02	Interior Fit Out and Finishes: including Doors
1.09	1.09.01	1.09.01.02	1.09.01.02.03	Glazing / Windows
1.09	1.09.01	1.09.01.02	1.09.01.02.04	Bogies
1.09	1.09.01	1.09.01.02	1.09.01.02.05	Braking
1.09	1.09.01	1.09.01.02	1.09.01.02.06	Articulation
1.09	1.09.01	1.09.01.02	1.09.01.02.07	Traction Motors
1.09	1.09.01	1.09.01.02	1.09.01.02.08	Coupling
1.09	1.09.01	1.09.01.02	1.09.01.02.09	Control and Communications
1.09	1.09.01	1.09.01.02	1.09.01.02.10	Auxiliary Equipment and Batteries
1.09	1.09.01	1.09.01.02	1.09.01.02.11	Heating, Ventilation and Air Conditioning
1.09	1.09.01	1.09.01.03		**Trailing Car**
1.09	1.09.01	1.09.01.03	1.09.01.03.01	Shell: including Painting
1.09	1.09.01	1.09.01.03	1.09.01.03.02	Interior Fit Out and Finishes: including Doors
1.09	1.09.01	1.09.01.03	1.09.01.03.03	Glazing / Windows
1.09	1.09.01	1.09.01.03	1.09.01.03.04	Bogies
1.09	1.09.01	1.09.01.03	1.09.01.03.05	Braking
1.09	1.09.01	1.09.01.03	1.09.01.03.06	Articulation
1.09	1.09.01	1.09.01.03	1.09.01.03.07	Traction Motors
1.09	1.09.01	1.09.01.03	1.09.01.03.08	Coupling
1.09	1.09.01	1.09.01.03	1.09.01.03.09	Control and Communications
1.09	1.09.01	1.09.01.03	1.09.01.03.10	Auxiliary Equipment and Batteries
1.09	1.09.01	1.09.01.03	1.09.01.03.11	Heating, Ventilation and Air Conditioning
1.09	1.09.02			**Freight Rolling Stock**
1.09	1.09.02	1.09.02.01		**Vehicle: state type**
1.09	1.09.02	1.09.02.01	1.09.02.01.01	Shell: including Painting
1.09	1.09.02	1.09.02.01	1.09.02.01.02	Interior Fit Out and Finishes: including Doors
1.09	1.09.02	1.09.02.01	1.09.02.01.03	Glazing / Windows
1.09	1.09.02	1.09.02.01	1.09.02.01.04	Bogies
1.09	1.09.02	1.09.02.01	1.09.02.01.05	Braking
1.09	1.09.02	1.09.02.01	1.09.02.01.06	Articulation
1.09	1.09.02	1.09.02.01	1.09.02.01.07	Traction Motors
1.09	1.09.02	1.09.02.01	1.09.02.01.08	Coupling
1.09	1.09.02	1.09.02.01	1.09.02.01.09	Control and Communications
1.09	1.09.02	1.09.02.01	1.09.02.01.10	Auxiliary Equipment and Batteries
1.09	1.09.02	1.09.02.01	1.09.02.01.11	Heating, Ventilation and Air Conditioning
1.09	1.09.02	1.09.02.01	1.09.02.01.12	Driver's Console and Cab Equipment
1.09	1.09.03			**Maintenance Operations: Rolling Stock**
1.09	1.09.03	1.09.03.01		**Vehicle: state type**
1.09	1.09.03	1.09.03.01	1.09.03.01.01	Shell: including Painting
1.09	1.09.03	1.09.03.01	1.09.03.01.02	Interior Fit Out and Finishes: including Doors
1.09	1.09.03	1.09.03.01	1.09.03.01.03	Glazing / Windows
1.09	1.09.03	1.09.03.01	1.09.03.01.04	Bogies
1.09	1.09.03	1.09.03.01	1.09.03.01.05	Braking
1.09	1.09.03	1.09.03.01	1.09.03.01.06	Articulation
1.09	1.09.03	1.09.03.01	1.09.03.01.07	Traction Motors

1.09	1.09.03	1.09.03.01	1.09.03.01.08	Coupling
1.09	1.09.03	1.09.03.01	1.09.03.01.09	Control and Communications
1.09	1.09.03	1.09.03.01	1.09.03.01.10	Auxiliary Equipment and Batteries
1.09	1.09.03	1.09.03.01	1.09.03.01.11	Heating, Ventilation and Air Conditioning
1.09	1.09.03	1.09.03.01	1.09.03.01.12	Driver's Console and Cab Equipment
1.09	1.09.04			**Engineering Operations Rolling Stock**
1.09	1.09.04	1.09.04.01		**Vehicle: state type**
1.09	1.09.04	1.09.04.01	1.09.04.01.01	Shell: including Painting
1.09	1.09.04	1.09.04.01	1.09.04.01.02	Interior Fit Out and Finishes: including Doors
1.09	1.09.04	1.09.04.01	1.09.04.01.03	Glazing / Windows
1.09	1.09.04	1.09.04.01	1.09.04.01.04	Bogies
1.09	1.09.04	1.09.04.01	1.09.04.01.05	Braking
1.09	1.09.04	1.09.04.01	1.09.04.01.06	Articulation
1.09	1.09.04	1.09.04.01	1.09.04.01.07	Traction Motors
1.09	1.09.04	1.09.04.01	1.09.04.01.08	Coupling
1.09	1.09.04	1.09.04.01	1.09.04.01.09	Control and Communications
1.09	1.09.04	1.09.04.01	1.09.04.01.10	Auxiliary Equipment and Batteries
1.09	1.09.04	1.09.04.01	1.09.04.01.11	Heating, Ventilation and Air Conditioning
1.09	1.09.04	1.09.04.01	1.09.04.01.12	Driver's Console and Cab Equipment
1.09	1.09.05			**Signalling Interface**
1.09	1.09.05	1.09.05.01		**Train Borne Equipment supplied by others**
1.09	1.09.05	1.09.05.01	1.09.05.01.01	Fit of Signalling Equipment: Supplier and European Traffic Management Requirements
1.09	1.09.06			**Testing and Commissioning**
1.09	1.09.06	1.09.06.01		**Testing**
1.09	1.09.06	1.09.06.01	1.09.06.01.01	Pre-delivery Testing
1.09	1.09.06	1.09.06.01	1.09.06.01.02	Post-delivery Testing
1.09	1.09.06	1.09.06.02		**Commissioning**
1.09	1.09.06	1.09.06.02	1.09.06.02.01	Commissioning
1.09	1.09.06	1.09.06.02	1.09.06.02.02	Handover
1.09	1.09.07			**Spares and Maintenance**
1.09	1.09.07	1.09.07		**Spares**
1.09	1.09.07	1.09.07	1.09.07.01.01	Initial Spares
1.09	1.09.07	1.09.07	1.09.07.01.02	Maintenance Spares
1.09	1.09.07	1.09.07.02		**Maintenance**
1.09	1.09.07	1.09.07.02	1.09.07.02.01	Service Agreement
1.09	1.09.07	1.09.07.02	1.09.07.02.02	Third Party Maintenance

Order Schedule 4 (Order Tender)