3.3 Benefits

The major benefits of delivering a new access planning system are listed below:

- Self serve booking – The Access Planning System will have the ability for a large percentage of work requests to be submitted and implanted into the access planning system with minimal input from the access team. In this case the access requester raises the access request.

- Early capture of data – The Access Planning System will have the ability to capture in a single place any information that describes potential work that may be required to take place and need access booked. This data can be made more detailed over time and enables much better visibility of planned work. Thus increasing the probability of successful access bookings.

- Single source/real time reporting – As all of the access data is contained within the access planning system at all states of evolution, it should be possible to generate report of the access requests at any time and for any duration of work and access requests from within the Access Planning System.

- Visualisations – The Access Planning System will contain multiple visualisations that can be used by both access requesters and planners to help plan more efficient access and speed up the overall access request process. These visualisations will be in the form of graphical real time views, maps, gant charts and calendar views.

- Automatic production of the NEPA, Engineering Notice and Possessions Plan – The Access Planning System will be able to create complete reports for publication, if required from the data contained within the system.

- Integrated pathing of trains – The Access Planning System will contain enough information and business rules to be able to path engineering trains from a defined list of pre planned paths. This feature gives significantly greater confidence in managing last minute changes of access and ensuring that the train pathing will still work.

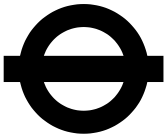
- Business led configuration management – The Access Planning System will contain the ability to modify in a controlled way the access related static data required to support the access planning. The configuration screens will enable updated underground geographic maps as well as data list within the system

3.4 To-Be Business Context

The business context diagram below shows all of the roles that would be expected to interact with the Access Planning System. For clarity and completeness, roles that have no interface with the Access Planning System have been included so that it is obvious that their functions are out of scope.

Many of the functions performed by the actors are listed below:

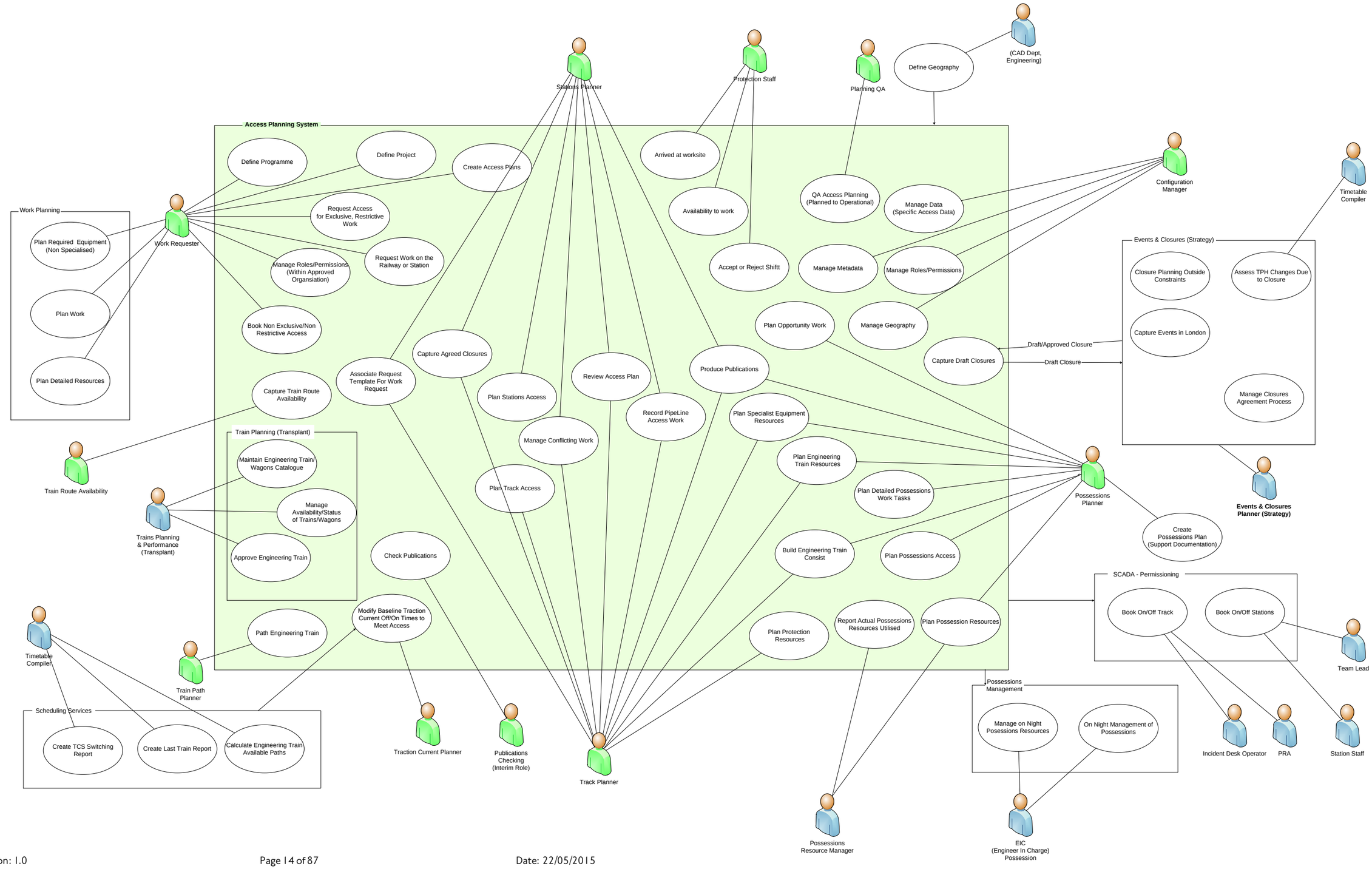
- Station Planner (Access Planner)
    - Capture Agreed Closures
    - Plan Stations Access
    - Manage Conflicting Work
    - Record Pipeline Access Work
    - Produce Publications
    - Associate Request Template for Work Request
- Track Planner (Access Planner)
    - Capture Agreed Closures
    - Plan Track Access
    - Manage Conflicting Work
    - Record Pipeline Access Work
    - Produce Publications
    - Plan Protection Resources
    - Plan Specialist Equipment Resources
    - Build Engineering Train Consist
    - Plan Engineering Train Resources
    - Associate Request Template for Work Request
- Possessions Planner (Access Planner)
    - Plan Opportunity Works
    - Produce Publications
    - Plan Protection Resources



    - Plan Specialist Equipment Resources
    - Build Engineering Train Consist
    - Plan Engineering Train Resources
    - Plan Detailed Possessions Work Tasks
    - Plan Possessions Access
- Traction Current Planner (Access Planner)
    - Modify Baseline Traction Current Off/On Times to Meet Access
- Train Path Planner (Access Planner)
    - Path Engineering Trains
- Train Route Availability (Access Planner)
    - Capture Train Route Availability
- Protection Staff
    - Update protection staff availability to work (ie on holiday)
    - Accept or reject shifts
    - Indicate they have arrived at the worksite
- Work Requester (Access Requester)
    - Request Access for Exc, Res Work
    - Request Work on Track or Station
    - Manage Roles/Permissions (Within Own Org)
    - Book Non Exclusive/Non Restrictive Access
- Configuration Manager
    - Manage Access Data
    - Manage Role/Permissions
    - Manage Geography
- Planning QA
    - QA Access Planning

- Approve Planned Access as Operationally Acceptable

- Publications Checking
  - Check Publications (Interim Role)


Access Planning System
Work Planning
Plan Required Equipment (Non Specialised)
Plan Work
Plan Detailed Resources
Work Requester
Define Programme
Define Project
Create Access Plans
Request Access for Exclusive, Restrictive Work
Request Work on the Railway or Station
Manage Roles/Permissions (Within Approved Organsiation)
Book Non Exclusive/Non Restrictive Access
Capture Train Route Availability
Associate Request Template For Work Request
Capture Agreed Closures
Stations Planner
Review Access Plan
Plan Stations Access
Manage Conflicting Work
Plan Track Access
Record PipeLine Access Work
Protection Staff
Arrived at worksite
Availability to work
Accept or Reject Shiftt
Planning QA
Define Geography
(CAD Dept, Engineering)
QA Access Planning (Planned to Operational)
Manage Data (Specific Access Data)
Manage Metadata
Manage Roles/Permissions
Manage Geography
Plan Opportunity Work
Produce Publications
Plan Specialist Equipment Resources
Plan Engineering Train Resources
Plan Detailed Possessions Work Tasks
Build Engineering Train Consist
Plan Possessions Access
Plan Protection Resources
Report Actual Possessions Resources Utilised
Plan Possession Resources
Configuration Manager
Timetable Compiler
Events & Closures (Strategy)
Closure Planning Outside Constraints
Assess TPH Changes Due to Closure
Capture Events in London
Manage Closures Agreement Process
Capture Draft Closures
Draft/Approved Closure
Draft Closure
Events & Closures Planner (Strategy)
Possessions Planner
Create Possessions Plan (Support Documentation)
Train Planning (Transplant)
Maintain Engineering Train/ Wagons Catalogue
Manage Availability/Status of Trains/Wagons
Approve Engineering Train
Train Route Availability
Trains Planning & Performance (Transplant)
Check Publications
Modify Baseline Traction Current Off/On Times to Meet Access
Path Engineering Train
Timetable Compiler
Train Path Planner
Scheduling Services
Create TCS Switching Report
Create Last Train Report
Calculate Engineering Train Available Paths
Traction Current Planner
Publications Checking (Interim Role)
Track Planner
SCADA - Permissioning
Book On/Off Track
Book On/Off Stations
Team Lead
Incident Desk Operator
PRA
Station Staff
Possessions Management
Manage on Night Posessions Resources
On Night Management of Possessions
Possessions Resource Manager
EIC (Engineer In Charge) Possession

3.4.1 As-is process

The diagram below shows the existing as-is process for access planning. Many systems are used to capture, plan and publish access within London Underground. The use of many systems causes many complications with the process of planning access, so are described below:

- Double and triple keying of information between systems
- Data being out of sync across systems at any one time
- Data being incorrectly keyed between systems
- High levels of checking required to ensure multiple data sources are correct
- Long lead time for publishing of data due to the data not being available for publishing until later in the process
- Many manual tasks are required as data is not in the correct format for rules to be applied until too late in the planning process.

Appendix E shows the 'Access As-Is Process Time Line' describing many of the timing constraints and lock down periods where data is required to be fixed past these points in time. As mentioned above most of these timings reflect the very manual process of planning that is undertaken today and the lack of a centralise database containing all of the planning information from concept through to on the night publishing.

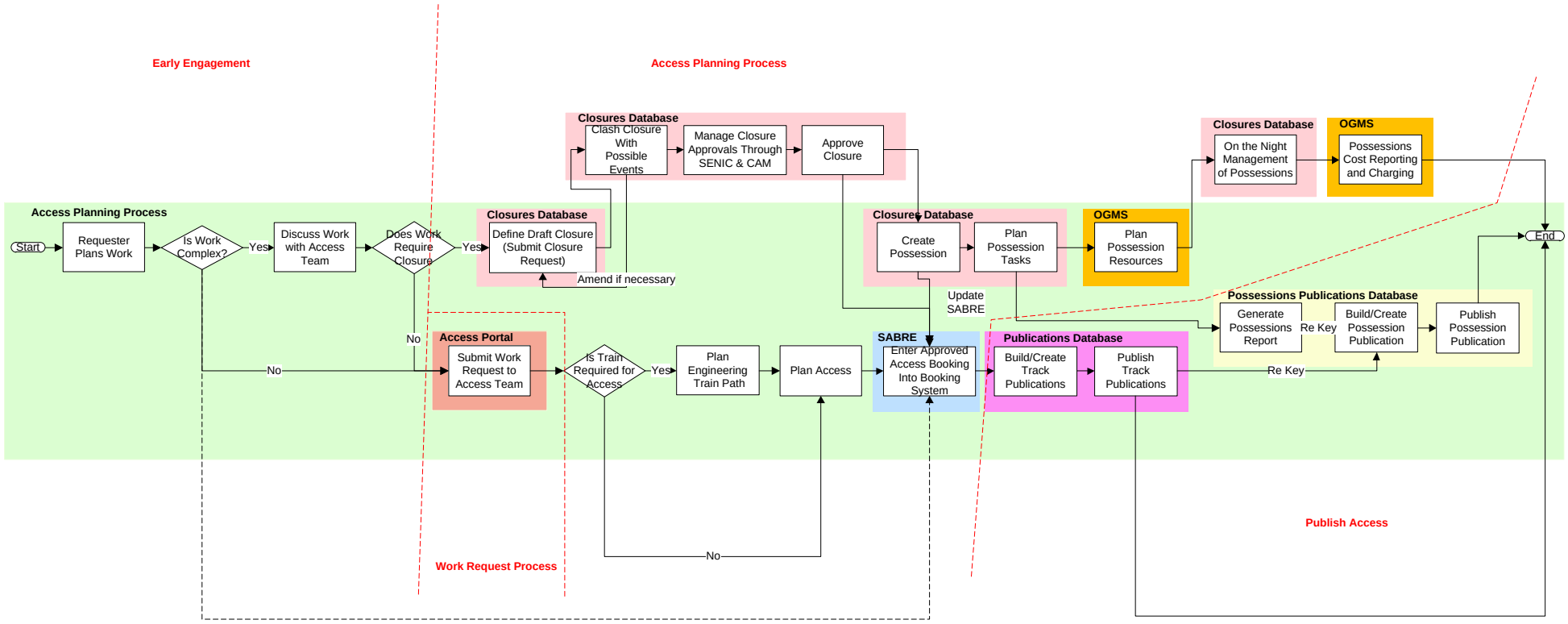


Figure 3-1, Access Planning As-Is Process

The following describes in more detail what is currently achieved at each stage of the Planning Process:

Early Engagement Process

Objective: To gain initial understanding of the approximate timescales, date(s) and type of work that is envisaged to be undertaken on the underground. In Addition it serves to provide the Access department with early visibility of any work that may be undertaken.

The current process involves:

- Early ideas of the scope of the proposed work to take place are presented to the access team for high level discussion.
- Initial feed back on the size, nature and rough time scales of the work proposed are evaluated. This evaluation is based on previous experience of similar work and other work occurring around the same location and time frame.
- Events and closures information that could significantly effect or hinder a work plan are discussed. Examples of such events are sporting events and Wembley, London bike ride, state visits, London Marathon etc.
- The proposed work is then redefined in work plans based on feedback from access department.
- Proposed work is assessed against possible viability of changes to long term timetables and operational services to support the work.
- At this point the potential new scope of the proposed work is more clearly known and less susceptible to change in the future. These long term plans can now be documented so that they are accommodated in the long term access work plans.

Work Request Process

Objective: To collect work requests from the requesters that contain key information around location, timings, constraints, type of work, impacts to the environment and other parties, plant and equipment and key personal information required to communicate with the requester.

Access Planning Process

Objective: To ensure that the planners can plan work and be kept informed of any changes to the work.

The access planner must take the total number of work requests and plan the required access to deliver the work in the most optimal way possible. Making efficient use of engineering trains (sharing train resources) specialist equipment (cranes etc), resources and multiple work type being carried out at the same sites and locations. The work types must be categorised into similar complexity and safety related work types. Business rules must be used to ensure the work is carried out in a safe a secure way. E.g. Asbestos removal work shall not be carried out along side other work. Simple litter

picking work can take place alongside track inspection work. Work shall be able to be manually planned where appropriate and aided by a planning tool if rules can be understood and reproduced. The planner should be able to make changes to existing plans and look at the effect of a change to other work plans occurring at similar times and locations. The planning process must take account of potential last minute changes and inform the relevant planners of such changes.

Publish Access

Objective: To communicate agreed access to a multi-discipline audience including maintenance and operational staff using appropriate media informing them of planned work to be undertaken on or around the track and stations for review.

Day of Operations (Access Control)

Objective: To allow contractors to safely book on and access track and station infrastructure.

The TAC use the information from the publications to update the base data in CTAC by dragging and dropping icons representing different hazard types on the maps held in the CTAC system.

The person in charge of the work group initially books on with the Station Supervisor, giving their work reference number (SABRE Number) and work party details. The Station Supervisor enters the number into the Permit Access System which verifies that it is valid on the day and location concerned. The person in charge fills out a evacuation register and declares their work parties are fit to work and are competent.

If the person in charge requires access to the track then they will call the TAC and, using the Solidus phone system, enter their SABRE and IV numbers on the phone keypad. CTAC pulls back pertinent works data from the SABRE system and, using the IV number, interrogates the SCL database to pull back the individual's competences.

This data is presented to the TAC on their CTAC screen when the individual's call is answered. The TAC and individual come to an understanding over where the work is taking place and which Traction Current Sections are needed to protect the work. The individual is informed of any additional hazards in the area and given a unique reference number and a call back time (the time by which they must have finished work, made the track safe and cleared with the TAC).

Once the work has been completed the person in charge will, if they accessed the track, clear the track of staff and equipment and then, via Solidus, clear their track booking. They will also book off with the Station Supervisor who will clear their booking in the Permit Access system.

Once CTAC informs the TAC that all persons are clear of a Traction Current Section then, just prior to it's switch on time, the TAC will contact the Power Controller and pass a 'line clear/line safe' message. This will allow the traction current to be switched back on again.

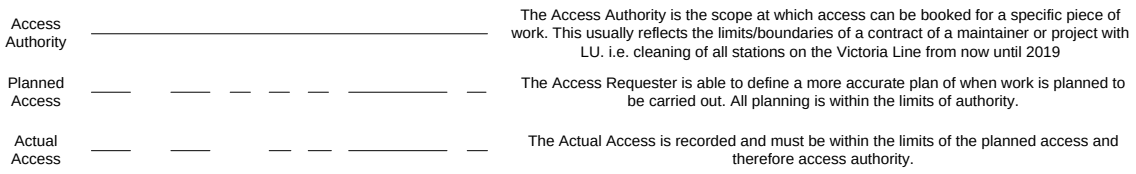
3.4.2 To-be process

The diagram below describes the main elements that a new planning system must meet to successfully deliver a new planning process for access. The new process is based around the concept capturing the access work by a means that is appropriate and relevant to the type of work it entails and the method of access protection the work requires. The process is described in more detail as follows:

- Programme
    - Each access request, however big or small will belong to a programme of works within London Underground. Major projects works and maintenance work all belong to a programme. At a programme level users will have to be given access to the system by either being requested by speaking to the access team or already created upon go live of the planning system.
    - Critical data for a programme will be captured including contact details and ownership
    - Programme owners will be given delegate responsibility to add projects and project owners
- Project
    - Each programme will have 1 or more projects
- Access Plans
    - Each project can have multiple access plans
    - Each access plan should describe a specific self-contained work type that is either a one off or repetitive. If an access plan is very high level and contains many elements of differing work and more importantly differing access, upon review by the access team the access plan may result in multiple work requests being made describe in the separate access requests.
- Access Team Review
    - Each Access Plan is reviewed by the Access Department and recommendations are made as to the possible methods of requesting access. I.e. An Access Plan may describe lots of different types of work. It may be recommended that the requester creates 3 unplanned requests and 2 planned requests using different forms.
    - The access department will associate an access plan element of access to an appropriate access request template. There will be different templates for requesting access. Some examples are:
        - Repetitive non-intrusive maintenance

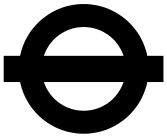
- Repetitive major track maintenance that requires a closure as the work will not fit into non traffic hours.
- Simple non-intrusive work i.e. cleaning on a station.
- Track work that requires the use of an engineering train
- …

- Access Work Request
  - The work requester will be able to request work using a predefined template that is applicable to the type of work and access required.
  - This work will be associated to an access plan, project and therefore programme.
  - This request will have a specific workflow and method of approval to ensure the work it describers can take place. This is achieved by allocating a workflow to a specific template.
  - Where work is simple and non-intrusive the system will enable the request to specify when and where the access will take place on the LU network. This is deemed to be the limit of access authority that the request has. I.e. the requester can now work on the track between the locations specified and between the dates listed in their request. See diagram below.
  - The requester can then choose to plan their access based on the limits of authority they have to work. This gives a greater and more accurate view of when they will be carrying out the work or activities. The actual access is then captured by the access control system(s) and work utilisation analysis can be made as the efficiency of the original access request.



See Appendix M for examples of access bookings and their corresponding access requests.

- Plan Access
  - The access is planned by either the planner or the access planning system may automatically plan the work based on some simple rules. See Appendix M for examples of access bookings and their corresponding access requests.
- Assurance of Access



- The access will have to be reviewed internally by qualified individuals and then approved as suitable for operational status.

- Publish Access
  - The access will be published when it is of status ‘operational’. This can be carried out with long periods of lock down, i.e. weeks as it is today or with hours or minutes lock down. This is to be determined and parameter based.

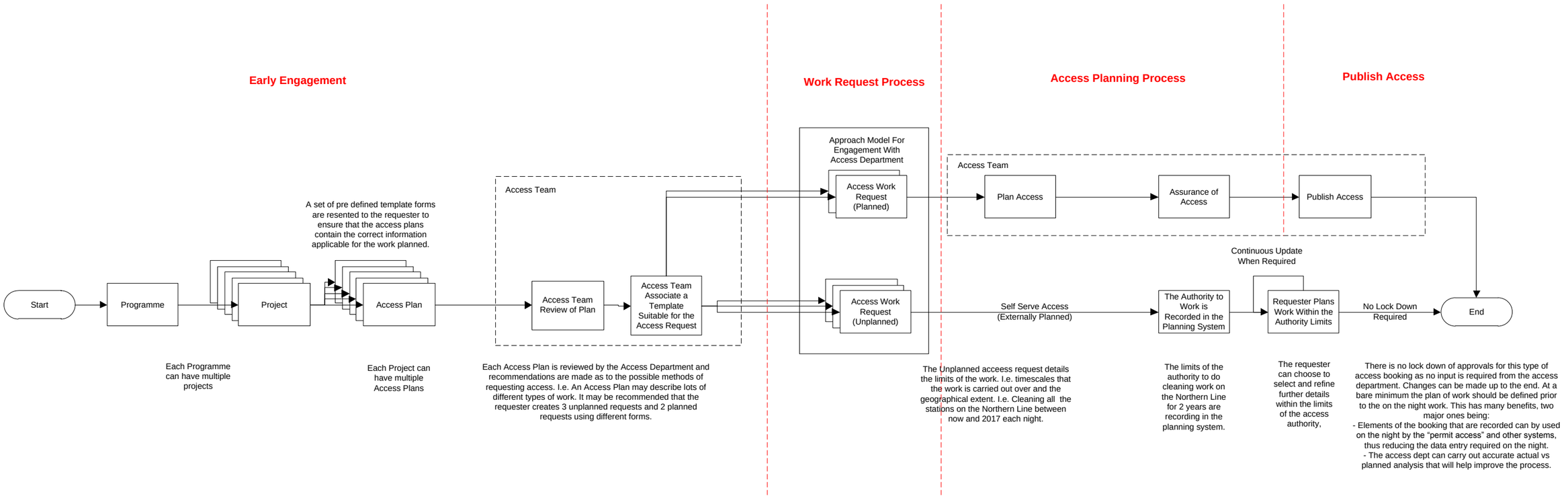


Figure 3-2, Access Planning To-Be Process

3.5 Systems Context

3.5.1 Systems Context – As-Is

The following context diagram shows the existing systems that support the access planning process. Currently the access planning process is delivered by many systems, some interfaced and others manually linked. The systems that exist within the access planning process are shown within the box 'Access Planning' shown.

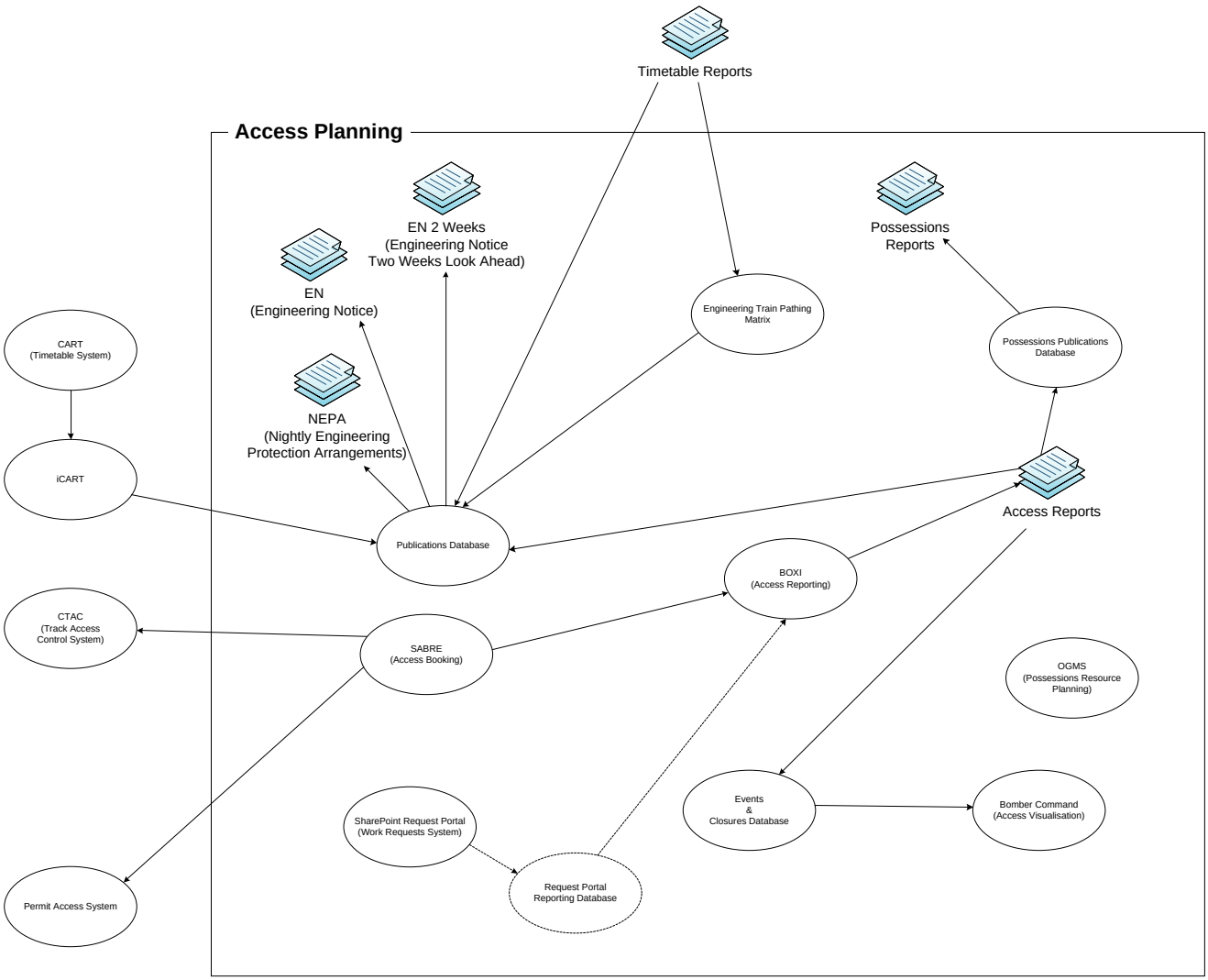


Figure 3-3, Access Planning As-Is System Context

3.5.2 Functional Process - To-be

The following diagram describes in further detail the main elements of the access planning system together with the functional components required to be delivered for each element of the system. The functional elements were created after analysing the different methods of planning that is required to be delivered by the new Access Planning System. The matrix in Appendix B 'Access Planning Options' shows the different planning options against the key drivers that define the different options. The matrix has been aligned to the existing access planning products that exist today as any future system will have to deliver a product of similar content.

Many steps are required to successfully deliver the different planning options. Many steps/functions are similar for multiple planning options. This is show in the matrix shown in Appendix C 'System Functions'. The matrix forms the basis of the main functional areas of all of the functional requirements defined in section 4 of this document. In both Appendix B and C the X denotes mandatory required and O, optional.

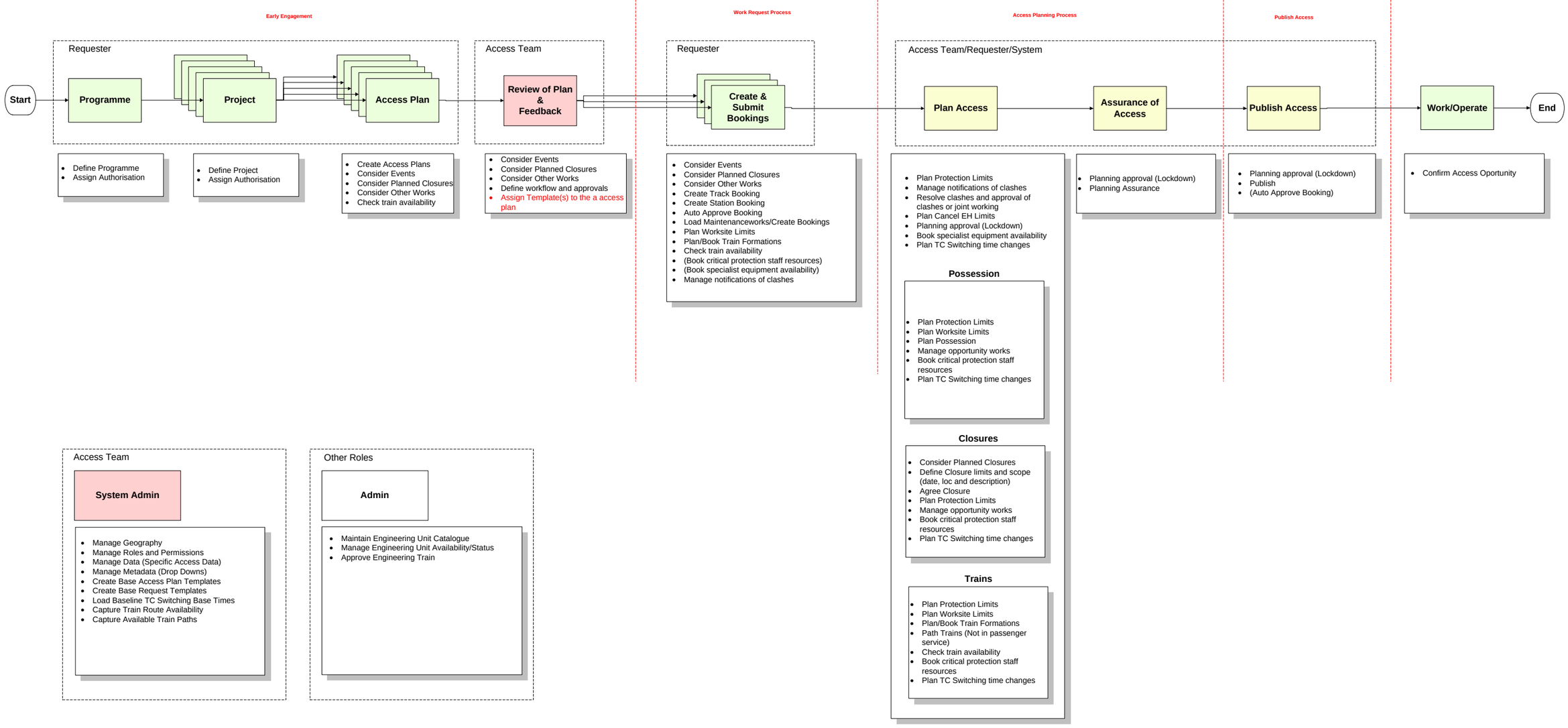


Figure 3-4, Access Planning To-Be Functional Process

3.5.3 Interfaces – To be

The New Access Planning System is required to interface to and from many systems to successfully deliver integrated access planning with London Underground (see diagram below). The ‘Closures System’ and ‘Events System’are shown as a dotted line as this could be delivered by the Access Planning System as well as by another external system using access planning data.

Over the next few years systems are being replaced in the access control area and so there will be a progressive migration from the systems today, towards the future operating model. The phasing out of existing systems and/or interfaces to and from the access planning system are shown in the diagram, in appendix D ‘Access Systems and Role Out’.

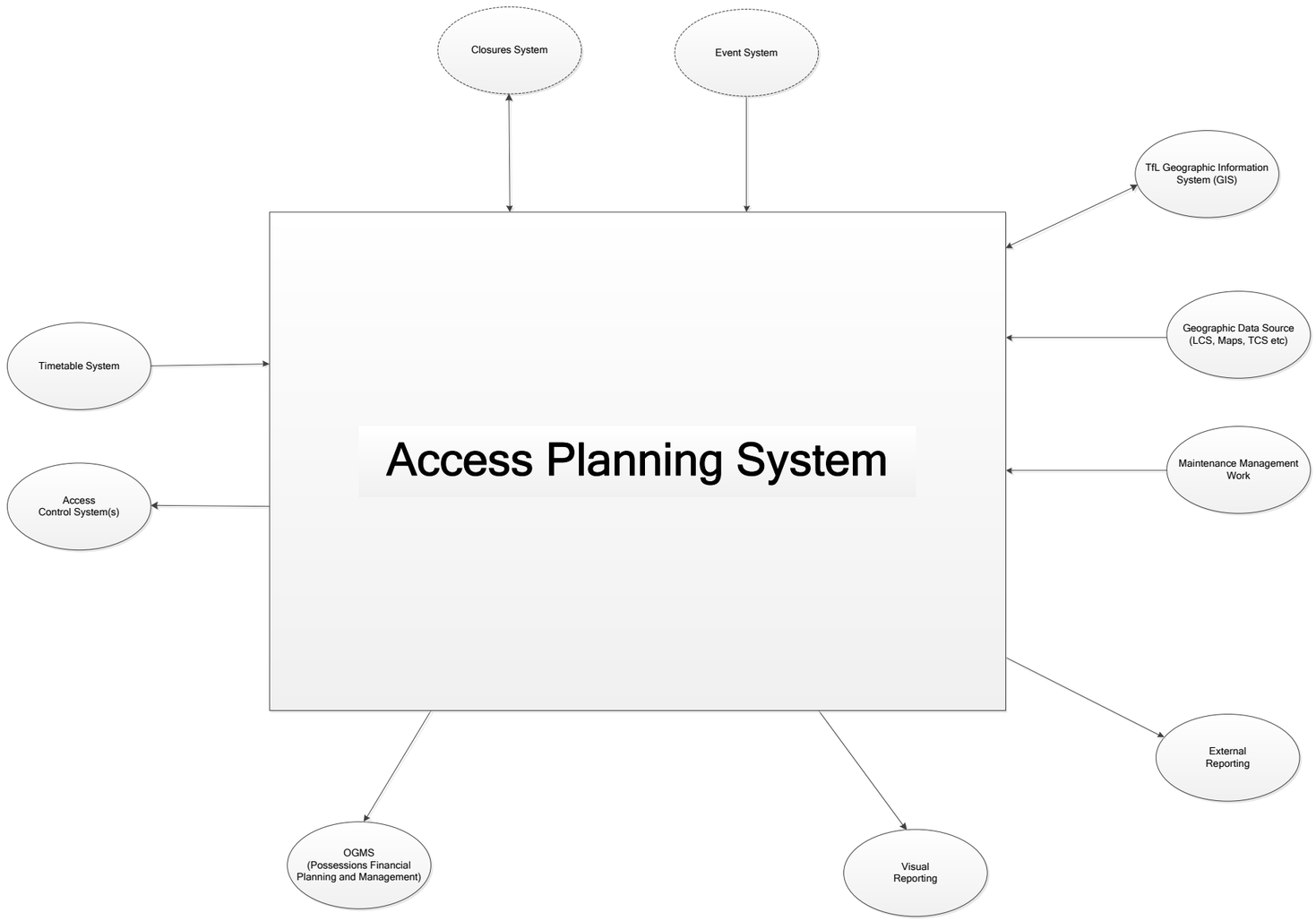


Figure 3-5, Access Planning To-Be Interfaces

4 Functional Requirements

The following section contains a list of the functional requirements resulting from workshops with the Access Transformation Team.

See the Included spreadsheet called '3A - Access Planning URS Functional Requirements.xls' for the complete list of the functional requirments for the access planning system.

NOTE: All references to data fields, report types, resource types, access catagories, are to aid explanation of the requirement, are not exhaustive and will be fully defined in the design phase

The requirements are categoried and tabulated in the following format:

- ID – This is a unique idetifier for each requirement.
- Type – This distinguishes headings from requirements.
- Phase – This is the high level phase that the requirements is required for within the access planning process. See Appendix C
- Function – This is a functional categorisation of the requirmenet. Note some requirements could exist in multipe functional areas. These requiremnets are not repeated. See Appendix C.
- Description - This is the requirement description.
- Classification - Requirements are classified into the following priority classifications
    - Must have – The solution must have this requirement in order to fulfil the scope of the project.
    - Should have – The requirement would be beneficial if it can easily be included in the solution.
    - Could have – This requirement will not be included with the solution but may be included at later a phase or subsequent project.
    - Wont have – The requirement is outside the scope of the project and not consistent with the objectives.
- Reference – This is a cross reference between the requirement and any information contained within the document or appendicies in the Access Planning URS.

5 Non Functional Requirements

The purpose of this section is to describe the Non functional requirements of the Access Planning System

See the Included spreadsheet called ‘3B - Access Planning URS Non Functional Requirements.xls’ for the complete list of the non functional requirments for the access planning system.

6 Constraints & Assumptions

The access planning department will have to operate “as normal” with no impact to the work planned to be carried out on the operational railway during the introduction of any new systems or processes.

A consistent geography can be determined from the highlighted data sources that are appropriate for the access system.

The external systems will continue to deliver the same information when the system goes live as they do today.

7 Current Systems

7.1 Within Access Planning System Scope

Access Portal

The Access Portal is a SharePoint site where access requests are captured for the LU infrastructure. The requests are made using a set of e-forms. The access planning team use the access request forms to create and plan access bookings within the SABRE system. The portal captures information such as:

- Work Details
- Timing for the work
- Location of the work
- Plant and Equipment required to complete the work
- Details of the work party involved with the completing the work

Closures Database

The closures database is currently contained within the wider Possessions Database. This MS Access Database enables railway and station closures to be defined in draft and managed through to approval.

SABRE

The SABRE (Site Access Booking for Rail Engineering) system is used to raise and handle the workflow of requests to access LU infrastructure resources. LUL infrastructure resources include track, station and vehicles; SABRE requests are generally raised by internal LU directorates and their subcontractors.

The SABRE system allows for requests for access to be reviewed, judged, accepted or rejected in the context of other requests and existing bookings.

SABRE is used to approve requests and once approval is granted on the SABRE system it implies that the requested access is considered to be booked.

Once booked, a party physically attends the booked station or track at the booked time to conduct requested work.

See Appendix L Ref-032 to Ref-037 for more background on the SABRE system.

Access Publications System

The Access Publications System is currently an MS Access database that receives last train, traction current off and on times and timetable information from the London Underground timetable system (CART). The system takes agreed planned engineering hours and possessions based information and generates a number electronic word and pdf publications that are used by many of the operational staff to manage and run track access on the underground network.

Possessions Publications Database

The possessions publications database enables possessions planners to capture possession planning information in a very structured way and publish the possessions being carried out in a MS Word based report that is used by operational and possessions based staff. See Appendix L Ref-042 for the user guide for the existing possessions database.

Possessions Database

The Possessions Database is an MS Access Database enables Possession Planners to capture the relevant information for the Possession Works Guide, ensuring the correct Application for Work Forms (AWFs), Worksites etc. are entered correctly and aligned to the delivery milestones.

BOXI

BOXI is the Business Objects reporting tool used by the access department to report on SABRE information.

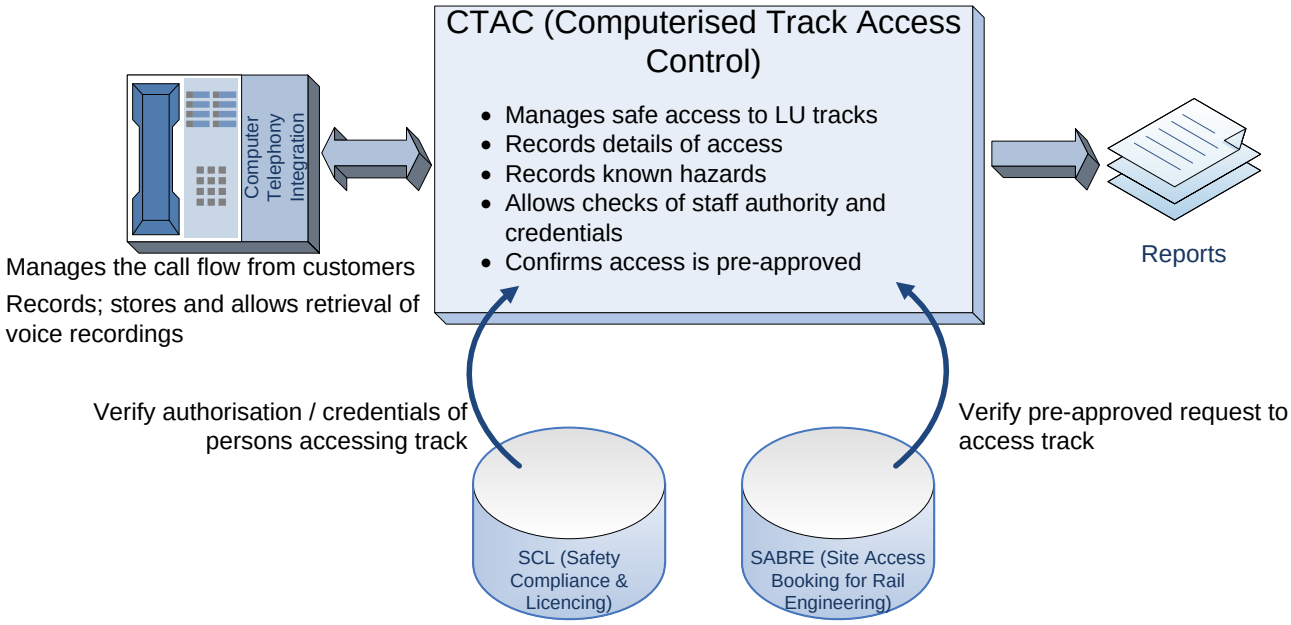
Bomber Command

Bomber Command (also known as "Access Visibility Tool" and "VSH@ctive" is an interactive map for sharing data across the business. The Access Department use Bomber Command to visualise SABRE bookings, Events and Closures information on a London Underground Beck map.

7.2 External to Access Planning Scope

CTAC

CTAC (Computerised Track Access Control) is a system used by LUL's TAC (Track Access Control) office to record and manage the safe and pre-approved booking of personnel onto and off of LU Track,



The application is integrated into a Telephony / Call Management & Distribution system that manages and prioritises the call flow from external customers into the TAC office, this interfaces with a Smartcall voice recording system which records; stores and allows retrieval of telephone voice recordings.

The CTAC System interfaces to the SABRE system to verify that a request for access is consistent with a pre-approved work package.

The CTAC system interfaces to the Safety, Critical Licensing (SCL) system to verify that the person requesting access to track, and protecting staff, has the appropriate current authorisation and credentials to do so.

Permit Access System

Permit Access utilises SABRE data and is designed for station staff to record actions and outcomes of site access visit requests made by LU Staff, Contractors and Sub-contractors. It provides a workflow around permitting staff access to stations. It assists station staff by returning confirmation if a SABRE number provided by subcontractor is valid. The system also records the outcome of station supervisor decisions, including time and date of permission granted and the person who granted permission.

Permit Access is also used to produce Denied Access Forms (DAFs), which are issued to personnel as a record that station staff denied access. It also produces Person In Charge Evacuation Register (PICER) which are issued when personnel are permitted access. The PICER contains information on personnel that would be needed in event of fire evacuation.

This service is considered to be business-critical and is used in Traffic and Engineering Hours

CART

The CART system, delivers business-critical functionality concerning the production of timetables and signalling outputs for the Operational Railway. The primary user interface of CART allows the creation of a timetable for a particular tube line.

RTS

RTS is a new railway timetabling system, which ultimately seeks to replace the existing CART (Computer Aided Railway Timetabling) system. RTS is business-critical and is the modern tool which timetable compilers will be using to produce timetables and signalling outputs to operate the railway.

OGMS

OGMS stands for Operations Group Management System. The OGMS database books and manages protection staff resources who are deployed onto the London Underground network in order to protect working environments. The database imports protection staff certification information in order to ensure staff are only booked on jobs where they have the necessary qualifications. The system interacts with an IVR telephone answering system which allows staff to book on and off from shift automatically. During shifts the system will record any issues, information on the progress of possessions, any complaints and incidents. At the end of each shift a detailed shift report is produced and circulated to interested parties. The system also provides financial information for accounting and charging purposes.

Appendix A: Glossary and Terms

Engineering Hours (EH)

Engineering Hours are overnight during which period the current is normally switched off and trains are not running.

Traffic Hours (TH)

Traffic Hours are day-time during which period the current is normally switched on and trains are running in passenger service.

Late Surrender Protection (LSP)

A method of providing protection for late running engineering works utilising buffer traction current sections and signals to ensure trains do not enter the area. This allows a train service to be operated around the affected area.

Public Information Systems (PIDs)
Passenger Information Displays (PIDs) are widely used to communicate messages to passengers on platforms regarding train services, expected arrivals and general customer announcements.

Traction Current Section (TCS)
There are 322 traction current sections across the LU network. These sections are switched off after the last published train has passed through the section (generally between 23:00 and 01:50 each night) and switched back on in the morning in time to allow the passage of the first train.

PWH-EH
The person undertaking the role of Protecting Workers on the Track during Engineering Hours

PRA
Person Requesting Access

TAC
Track Access Controller

TC
Traction Current

TCS
Traction Current Section

P-CRID
Permanent Current Rail Indicator Device

PCRO
Power Control Room Operator

Access Control System

The Access Control System is a term referred to by the Access Planning System and is meant to represent all of the systems used within the railway to manage the access onto stations and track. Today the access control systems use with London Underground are:

- Permit Access
- CTAC

In the future these systems will be replaced by the Permissioning System which will enable both station and track access to be requested and booked on the operational railway.

Case Management

For the purposes of access planning, case management is defined as the following.

To allow for each access plan, work request, possession plan and closure:

- Assigning the item to an individual access planner or access planning team
- Keep a record of changes to the item including status changes
- Keep a record of the access planners who have worked on the item
- Keep a log of meeting notes and actions for meetings related to the item
- Keep a log of comments and notes raised on the item as it progresses through its lifecycle
- Ability to attached associated documents to an item. E.g. emails, documents and pictures
- Ability to links external documents to an item
- Manage a task list associated with an item
- Expose and show time scale lockdown and calendar milestones.

Appendix B: Access Planning Options

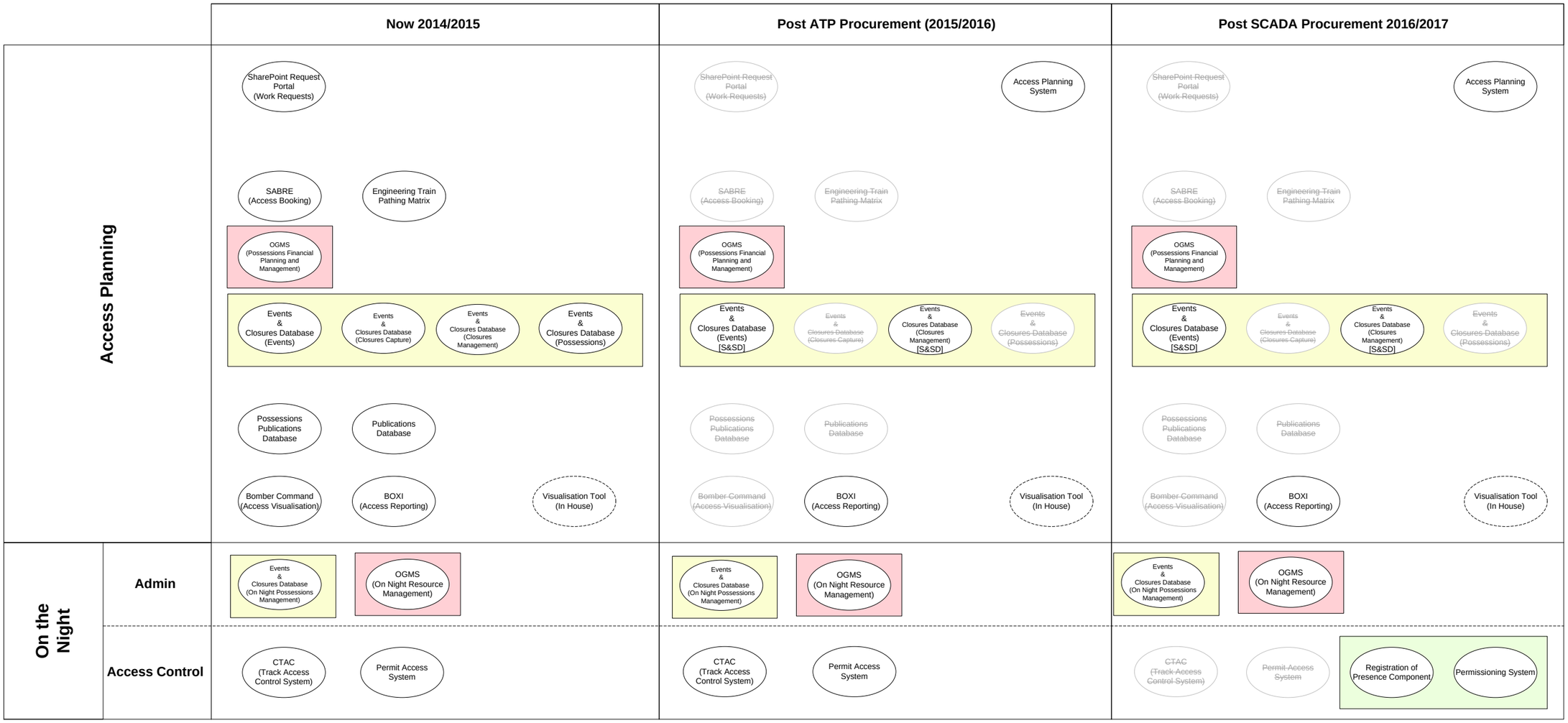
Planning Options										Planning Products												
Planning Name		**Track**	**Station**	**Trains**	**Closure**	**Possession/SA/ECA**	**Restrictive**	**Exclusive**			**Permit Access**	**Permissioning (Track)**	**Station Work Plan**	**2 Week EN Look Ahead**	**Engineering Notice**	**NEPA**	**Possessions Plan**	**10 Week Review**	**CAM Closure Approval**	**Trains Meeting**	**Altered TC Times**
Simple Track booking	**1a**	X								**1a**	X	X									
Simple Station Booking	**1b**		X							**1b**	X		X								
Simple Track & Station Booking	**1c**	X	X							**1c**	X	X	X								
Restrictive Track Booking	**2a**	X					X			**2a**	X	X				X		X			
Restrictive Station Booking	**2b**		X				X			**2b**	X		X								
Restrictive Track & Station Booking	**2c**	X	X				X			**2c**	X	X	X			X		X			
Exclusive Track Booking	**2e**	X						X		**2e**	X	X				X		X			
Exclusive Station Booking	**2f**		X					X		**2f**	X		X								
Exclusive Track & Station Booking	**2g**	X	X					X		**2g**	X	X	X			X		X			
Track Closure	**3a**	X			X					**3a**	X		X						X		
Station Closure (Major)	**3bi**		X		X			X		**3bi**	X		X						X		
Station Closure (L&E)	**3bii**		X		X					**3bii**											
Station Closure (Minor)	**3biii**		X		X					**3biii**											
Track & Station Closure	**3c**	X	X		X					**3c**	X		X								
Engineering Hours Possession	**4**	X				X				**4**	X	X		X	X	X	X	X			
EH&TH Possession	**5**	X			X	X				**5**	X	X		X	X	X	X	X	X		X
Track Eng Hours Possession With Train	**6**	X		X		X				**6**	X	X		X	X	X	X	X		X	X
Track & Station Eng Hours Possession With Train	**7**	X	X	X		X				**7**	X	X	X	X	X	X	X	X		X	X
Track & Station Eng Hours Possession With Train Within Closure	**8**	X	X	X	X	X				**8**	X	X	X	X	X	X	X	X	X	X	X
Stock Moves	**10**			X						**10**				X	X	X		X		X	X
Cancel Engineering Hours	**11**	X						X		**11**		X		X	X	X		X			X
Cancel Engineering Hours With Trains	**12**	X		X				X		**12**		X		X	X	X		X		X	X
Maintenance Work	**13**	X	X	X	X	X	X	X		**13**	X	O	O	O	O	O	O	O	O	O	O
											Don't	**Do care for planning**									

Appendix C: System Functions

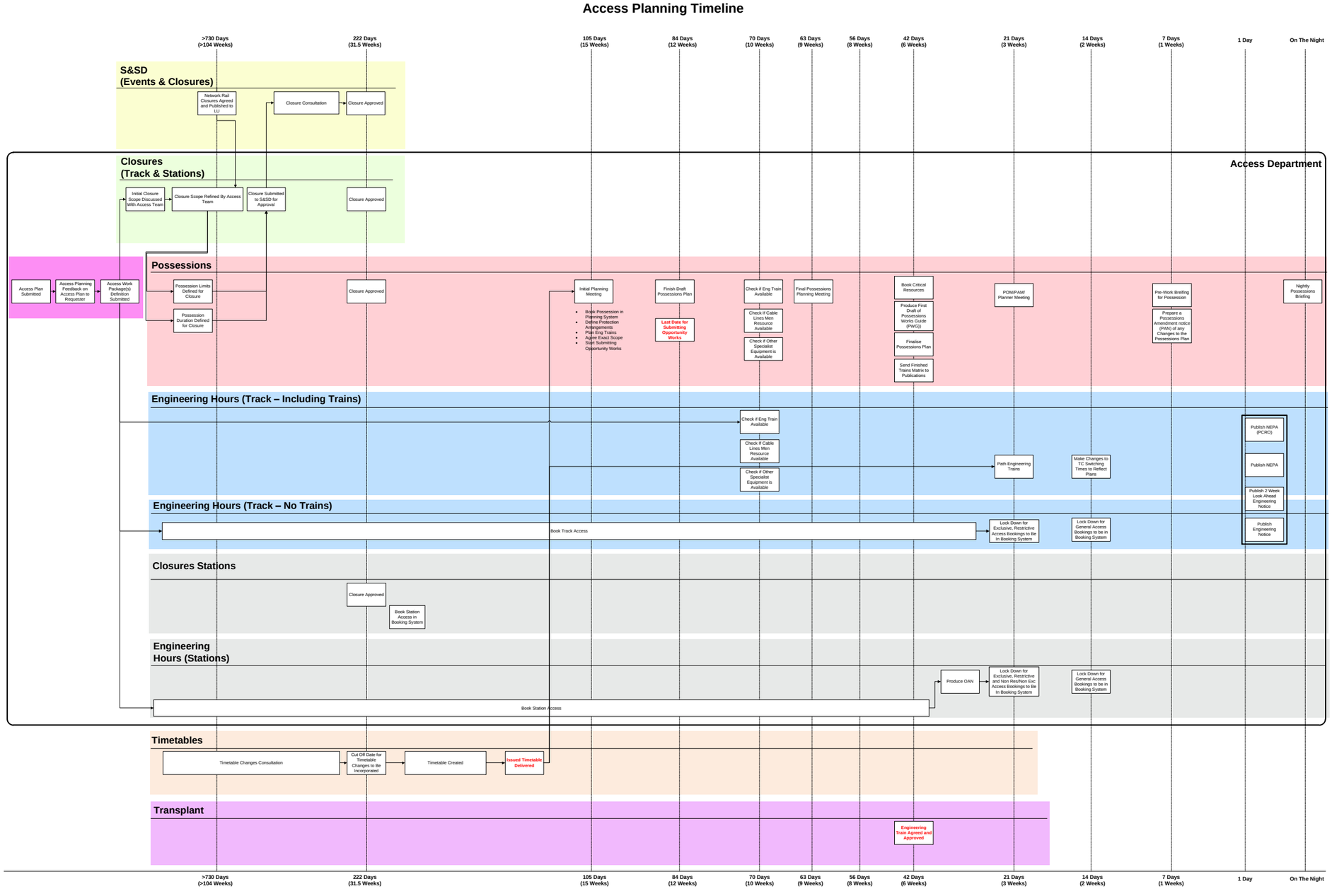
		Data Capture					Access Planning																						Approval		Publish	On Night
Planning Name		**Define Programme**	**Define Project**	**Create Access Plans**	**Assign Authorisation**	**Create and Allocate Templates**	**Consider Events**	**Consider Other Works**	**Create Track Booking**	**Create Station Booking**	**Define workflow and approvals**	**Define Closure limits and scope (date, loc and description)**	**Agree Closure**	**Auto Approve Booking**	**Load Maintenanceworks/Create Bookings**	**Plan Protection Limits**	**Plan Worksite Limits**	**Plan Cancel EH Limits**	**Plan Possession**	**Plan/Book Train Formations**	**Path Trains (Not in passenger service)**	**Manage opportunity works**	**Check train availability**	**Book critical protection staff resources**	**Book specialist equipment availability**	**Manage notifications of clashes**	**Resolve clashes and approval of clashes or joint working**	**Plan TC Switching time changes**	**Planning approval (Lockdown)**	**Planning Assurance**	**Publish**	**Confirm Access Oportunity**
Simple Track booking	**1a**						O	X	X		X			O		X	X							O	O	X					X	X
Simple Station Booking	**1b**						O	X		X	X			O			X									X					X	X
Simple Track & Station Booking	**1c**						O	X	X	X	X			O		X	X							O	O	X					X	X
Restrictive Track Booking	**2a**						O	X	X		X			O		X	X							O	O	X	X		X	X	X	X
Restrictive Station Booking	**2b**						O	X		X	X			O			X									X	X		X	X	X	X
Restrictive Track & Station Booking	**2c**						O	X	X	X	X			O		X	X							O	O	X	X		X	X	X	X
Exclusive Track Booking	**2e**						O	X	X		X			O		X	X							O	O	X	X		X	X	X	X
Exclusive Station Booking	**2f**						O	X		X	X			O			X									X	X		X	X	X	X
Exclusive Track & Station Booking	**2g**						O	X	X	X	X			O		X	X							O	O	X	X		X	X	X	X
Track Closure	**3a**						X	X	X		X	X	X									X				X	X		X	X	X	
Station Closure (Major)	**3bi**						X	X		X	X	X	X									X				X	X		X	X	X	
Station Closure (L&E)	**3bii**																														X	
Station Closure (Minor)	**3biii**																														X	
Track & Station Closure	**3c**						X	X	X	X	X	X	X									X				X	X		X	X	X	
Engineering Hours Possession	**4**						O	X	X		X					X	X		X			X		X	O	X	X		X	X	X	X
EH&TH Possession	**5**						X	X	X		X	X	X			X	X		X			X		X	O	X	X	X	X	X	X	X
Track Eng Hours Possession With Train	**6**						O	X	X		X					X	X		X	X	X	X	X	X	O	X	X	X	X	X	X	X
Track & Station Eng Hours Possession With Train	**7**						O	X	X	X	X					X	X		X	X	X	X	X	X	O	X	X	X	X	X	X	X
Track & Station Eng Hours Possession With Train Within Closure	**8**						X	X	X	X	X	X	X			X	X		X	X	X	X	X	X	O	X	X	X	X	X	X	X
Stock Moves	**10**						X	X			X			O						O	X		O	O		X	X	X	X	X	X	X
Cancel Engineering Hours	**11**							X										X								X	X	X	O	X	X	
Cancel Engineering Hours With Trains	**12**							X										X		O	O		O			X	X	X	O	X	X	
Maintenance Work	**13**						X	X	X	O	X	O	O	O	X	O	O	O	O	O	O	O	O	O	O	O	O	X	O	X	X	X	

Not Applicable

Appendix D: Access Systems and Role Out



Appendix E: Access As-Is Process Time Line



Appendix F: Access Planning Visualisations

The following screen shots are taken from an access visualisation proof of concept that has been used to stimulate conversation around how track and station visualisation tool can be used for both access requests and access planning. The screen shots are included to show possible methods of visualising access data and related events and closures. The examples shown below contain three different data sources:

- SABRE Booking information (Track and Station bookings)
- Events information
- Closures information

An access requester would use many of these visualisations to find possible locations and dates where no work is taking place and so enable them to successfully manage their work and bookings.

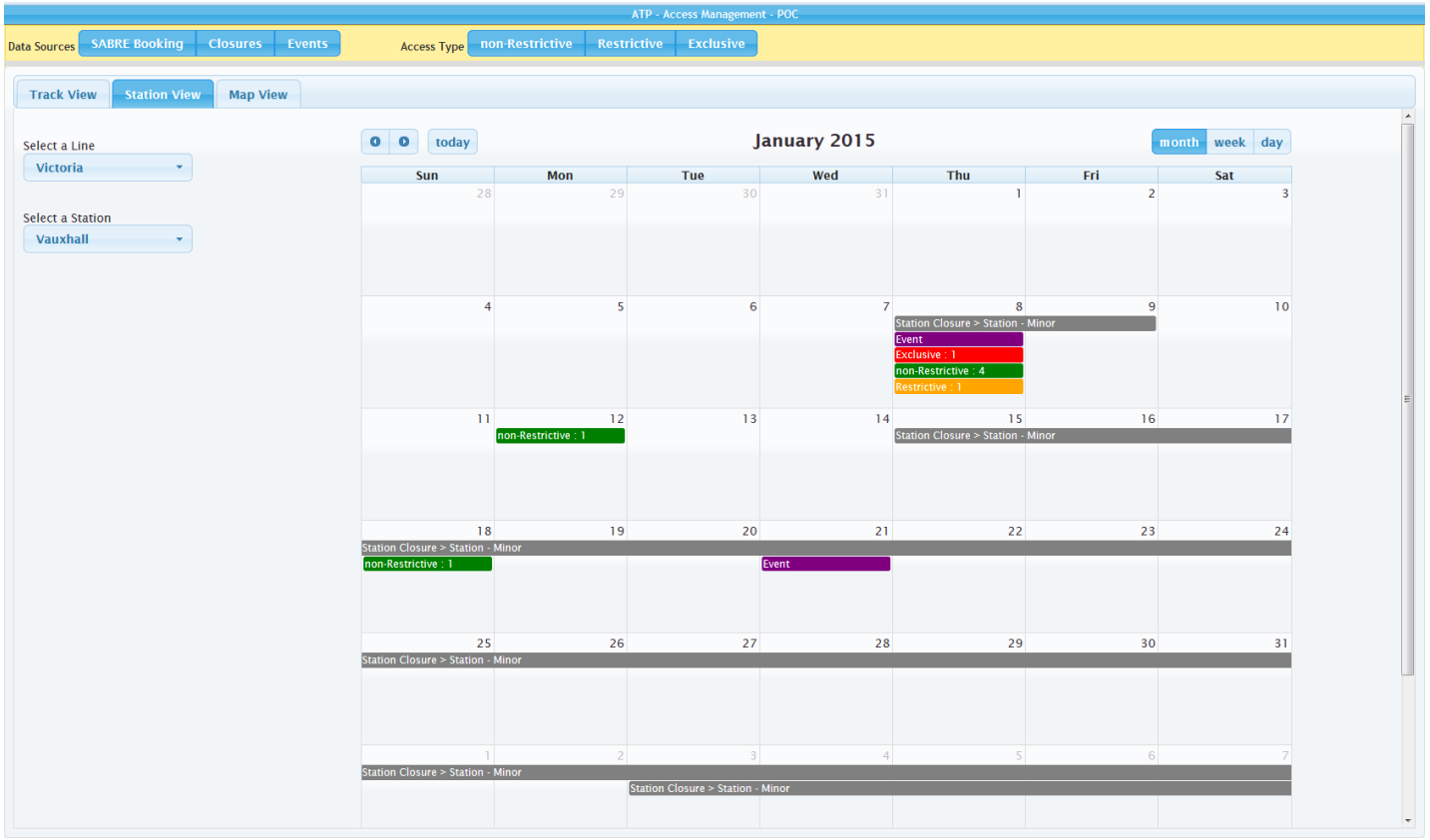
All of the visualisations below have the ability to filter the source data on of off and filter the access types (exclusive, restrictive, non restrictive/non exclusive)

F1 Station View

The Station View is very much used for Station requests and stations booking management. An individual requesting access to a station may choose to use this visualisation to check if there are any other bookings present at the same time and location. The requester will also need to know if there are any station closures or events on in London that could affect or cause the booking to be cancelled or not allowed. The access planner would use the station view to look at possible cashes of work. The access planner would use the calendar view to quickly find gaps in work to make better use of access within London Underground.

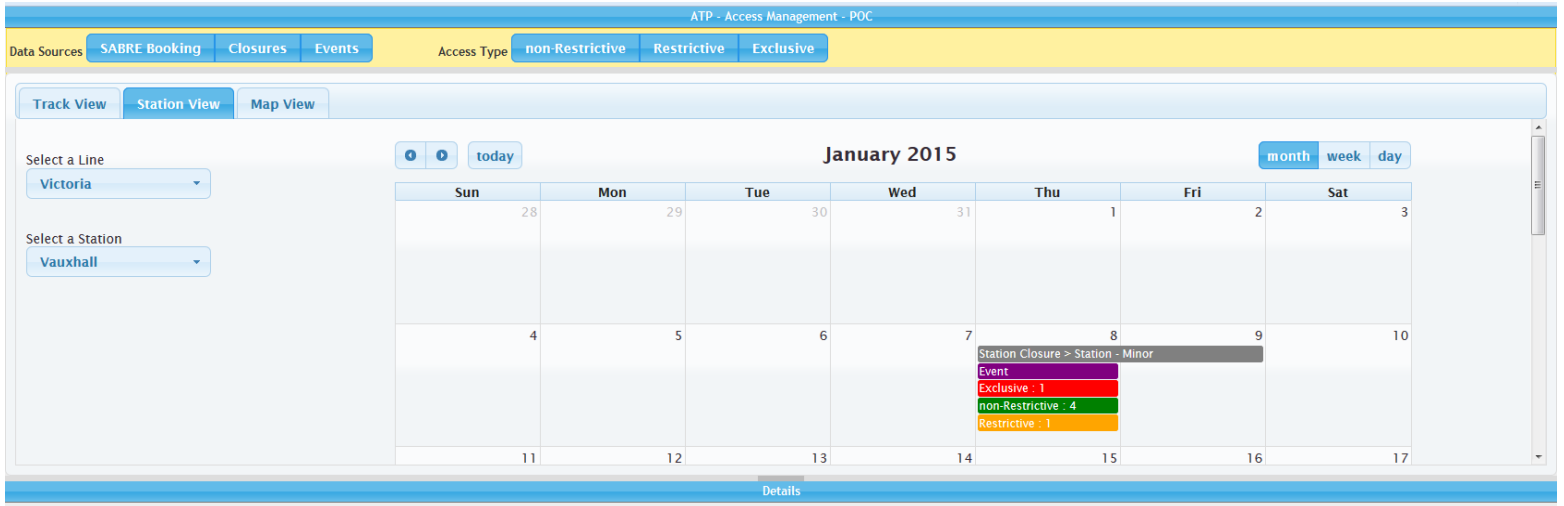
F1.1 Calendar View - Calendar

Using the calendar view the user can navigate through the calendar months to look for either other bookings or potential spaces for bookings. The number of bookings present on a given day for a given location calendar shall be shown as a count of the number of bookings. A RAG status has been applied to these booking to show the access type (Exclusive, Restrictive, Non Exc/Non Rest).



F1.2 Calendar View – Booking Details

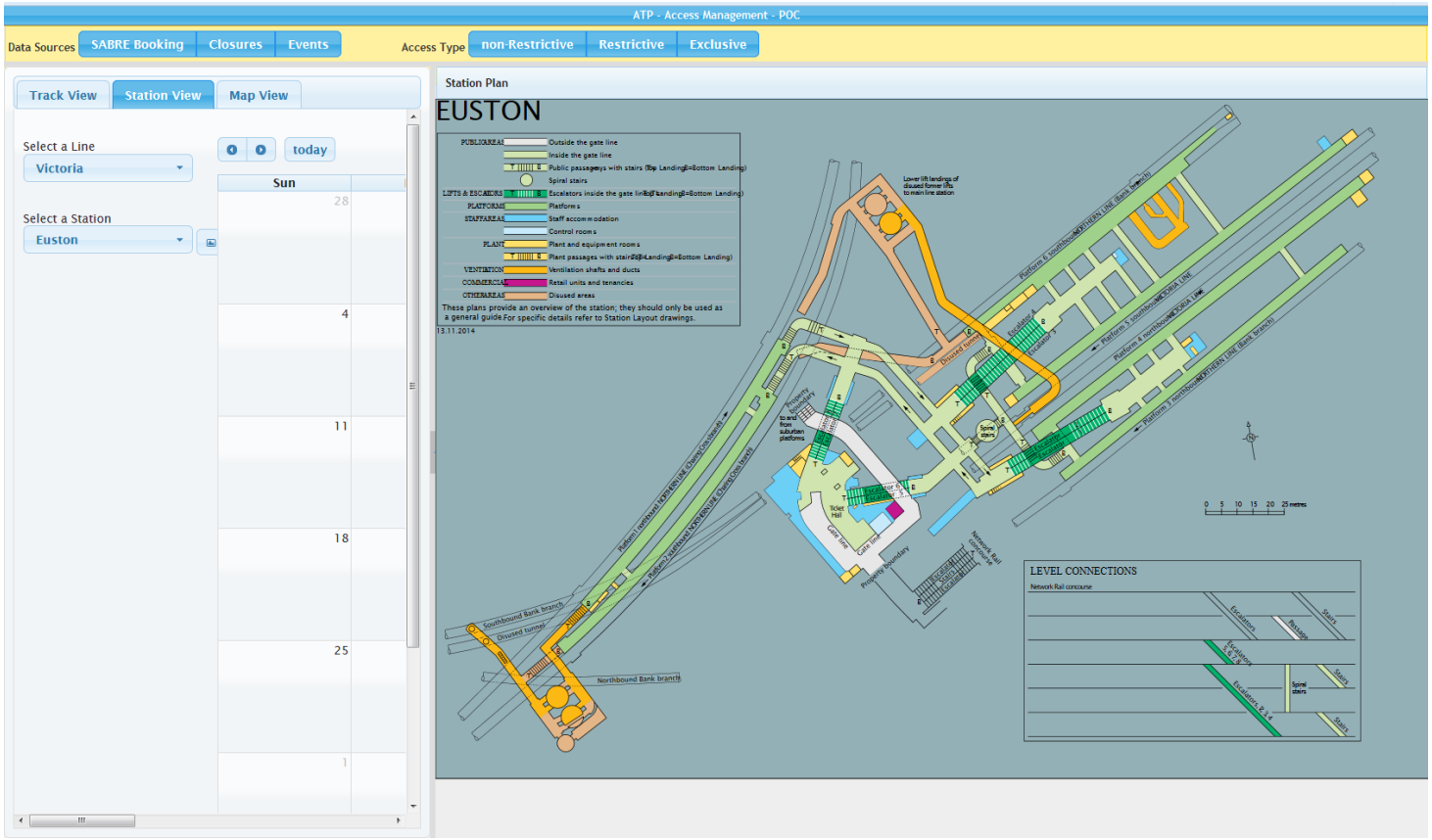
Each booking can be drilled down further to show the underlying records describing the bookings. Ach field within the detailed view is able to be sorted.



Sabre Number	Request Set Status	Station Shift Date	Station User Summary	Category of Work	Station Booking Type	Station Status	SID CODE	SID Description	Station Purpose Of Access	Station Work Methods	Accountable Manager	Accountable Manager Phone Number
2328689	Completed	2015-01-08	VAUXHALL:Construction of new lift shaft/stairways/lift electrical equip rm, gateline, reconfiguration of ticket hall/boh areas-incl. station accom/welfare, Station Control Facility/Offices/POM room/secure suite), provision of temporary station facilities, electrical isolations, cleaning of existing brickwork, new floor surfaces, new gates, site fire hoardings, ATM/secure room, advertisings supplies, temporary services to maintain full station facilities during the works. WORK AREAS: ALL AREAS	Upgrade/Renewals /Project	Non-Exclusive / Non-Restrictive	Completed	3/411	STORE	Premises '&' structures	Intrusive Survey	MARK SWEETMAN	7515052541
2329805	Approved	2015-01-08	VAUXHALL - VAUXHALL STATION (LUL) MODERNISATION, SCR ROOM 3/746	Installation/Removal	Non-Exclusive / Non-Restrictive	Withdrawn	2/661	SWITCH ROOM E1	Auto Fare collection	Replace	BOB JAMIESON	07788 568892
2333530	Approved	2015-01-08	Intrusive survey of Platforms 1 & 2 VAUXHALL	Upgrade/Renewals /Project	Restrictive	Approved	2/732	CER - ESCALATORS 1 3	Premises '&' structures	Refurbishment	Mark Sweetman	07515 052541
2333557	Approved	2015-01-08	Vauxhall Station Project enabling works including removal of wall panels/signage/tiling/concrete infills for shaft and breakthrough works, installation of hoardings, surveys including confined space working. Relocation of existing services to facilitate project works. (Access via Main Ticket Hall, escalators 1-3 to Platforms 1 and 2). Sub Cont: Bechtel Ltd - Hani Rizkallah, Murphys, JGL.	Upgrade/Renewals /Project	Non-Exclusive / Non-Restrictive	Approved	2/001	BOOKING HALL	Premises '&' structures	Refurbishment	Mark Sweetman	07515 052541
2334229	Approved	2015-01-08	VAUXHALL STATION (LUL) MODERNISATION	Upgrade/Renewals /Project	Exclusive	Approved	2/151	UMC - ESCALATORS 1 3	Premises '&' structures	Refurbishment	Mark Sweetman	7515052541
2334328	Approved	2015-01-08	VICTORIA LINE - VAUXHALL BAU PROJECT DUEL OUTLET INSTALLATION	Upgrade/Renewals /Project	Non-Exclusive / Non-Restrictive	Approved	3/407	CLEANING SERVICES - STAFF ROOMS	Comms	Hand Tools	DAVE HENSON	01189 699 777

F1.2 Station Plan

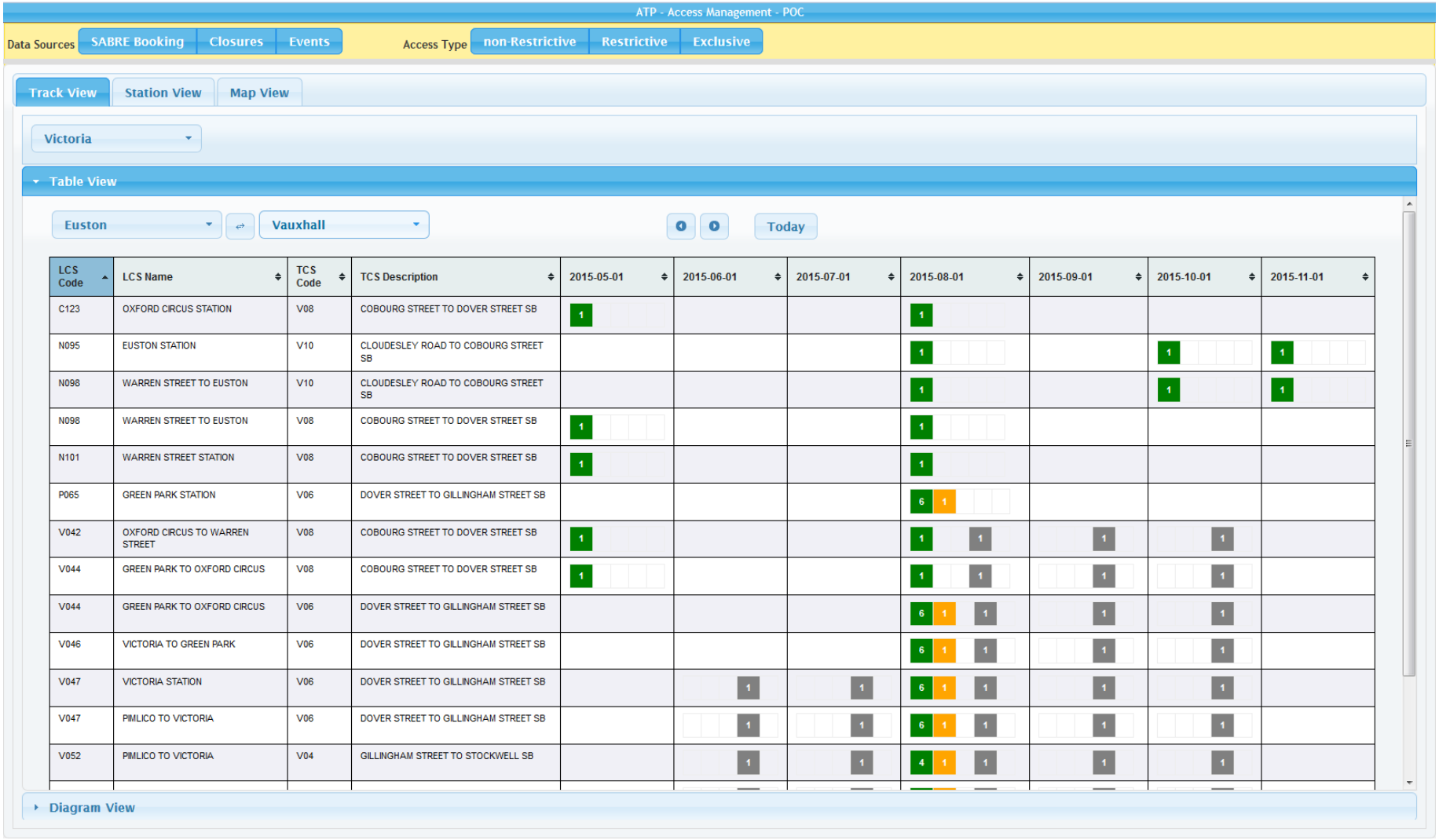
Areas of each station are broken down into zones and sometimes specific rooms and locations i.e. escalator 1, escalator 2, platform 1, platform 2, concourse etc. The amount of work present in each of these areas can be plotted on the station plans with the ability to drill down to the specific booking records for a selected area/zone.



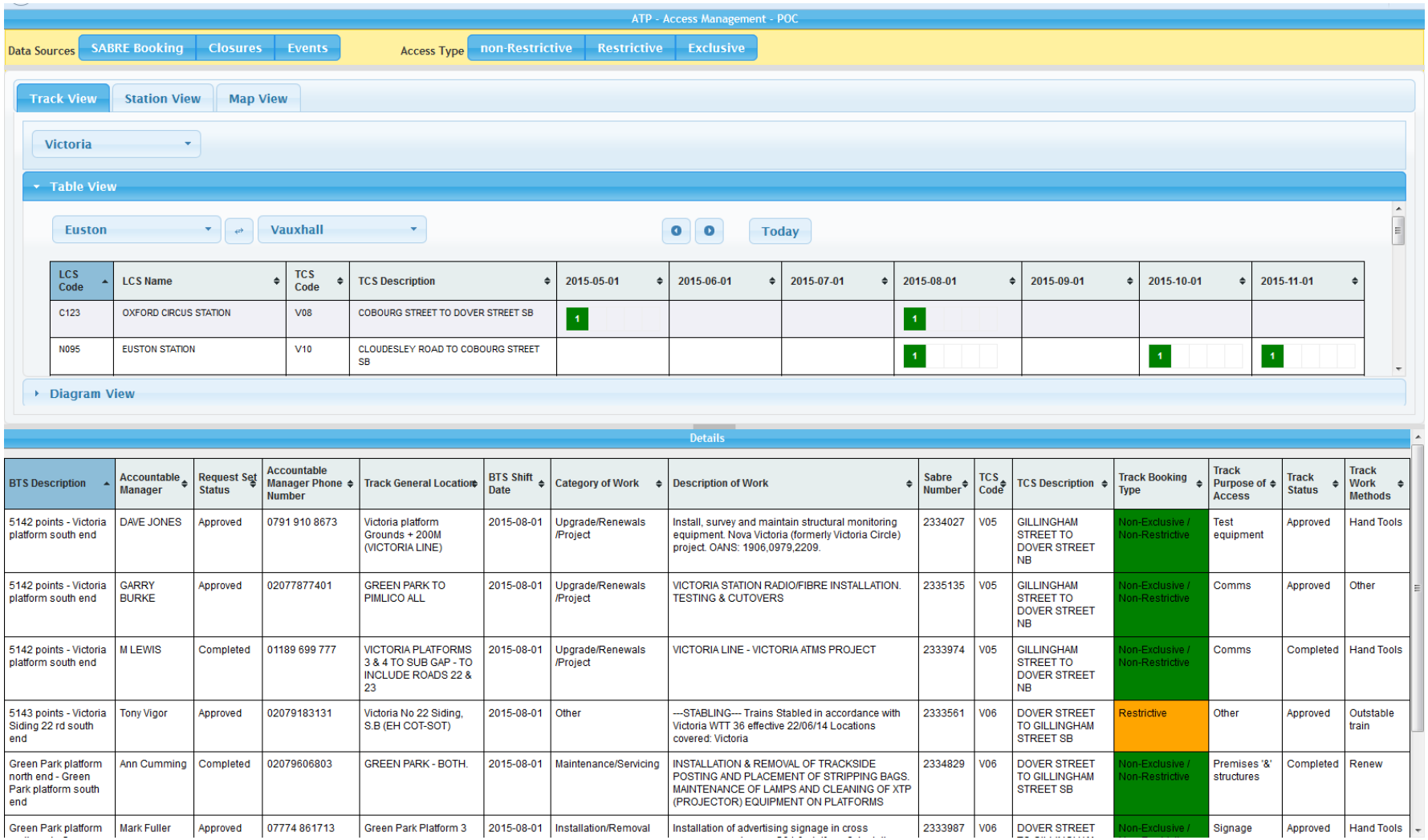
F2 Track View

F2.1 Table View (Gant View)

The Track table view is a method of displaying the booked work, events and closure information for a given week on one single screen/report against the traction current sections of an underground line. The view enables the user to filter the section between two station locations and change the week forwards and backwards. The ability to look at different dates enables' the user to quickly scan through the calendar and look for potential clashes or allocations and times where no work is occurring. Where access bookings are present there is a count of the number of bookings of a given access type shown in the relevant day and TC section. The user is able to click on the count and then see all of the bookings for that selected day.



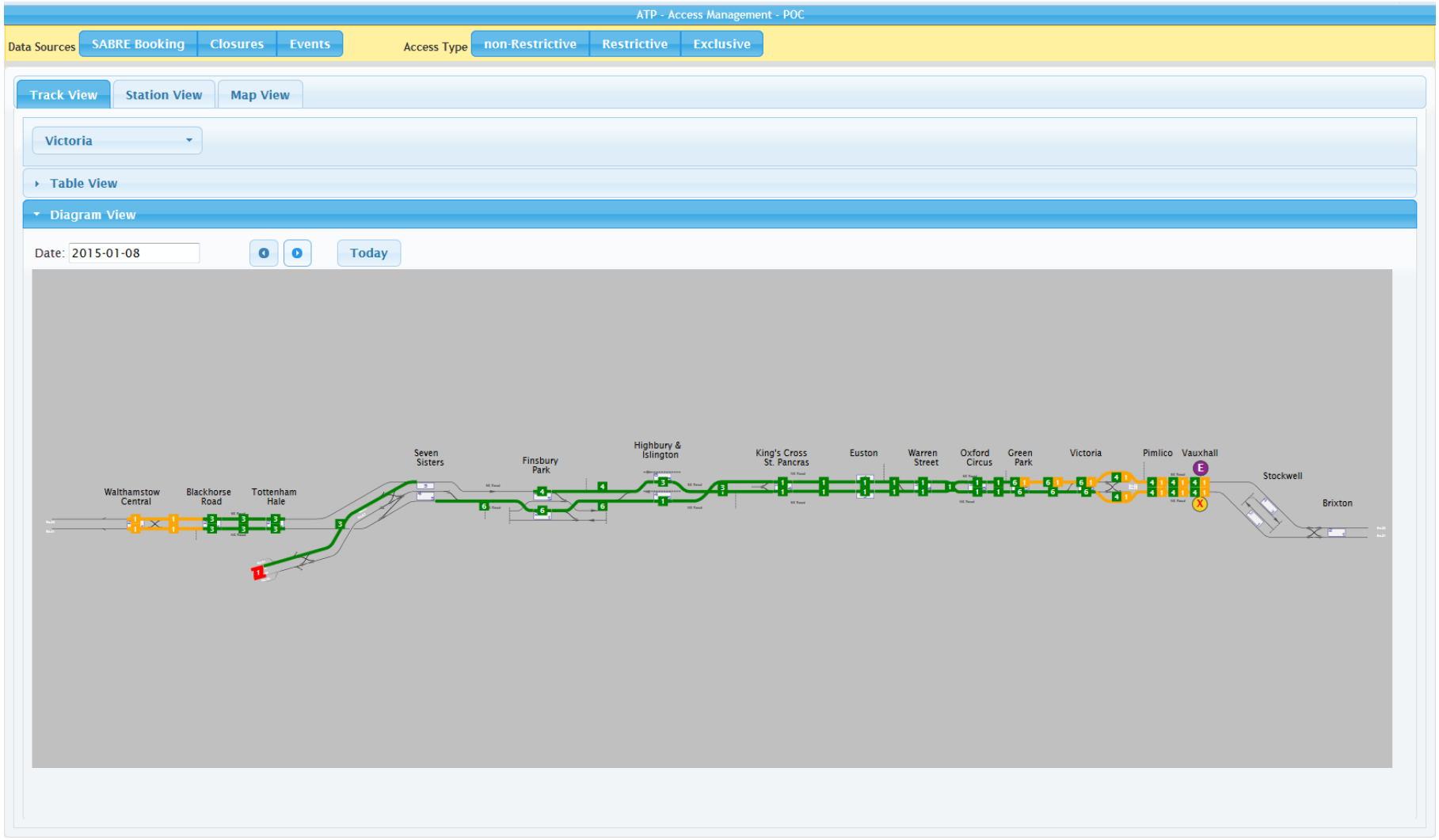
LCS Code	LCS Name	TCS Code	TCS Description	2015-05-01	2015-06-01	2015-07-01	2015-08-01	2015-09-01	2015-10-01	2015-11-01
C123	OXFORD CIRCUS STATION	V08	COBOURG STREET TO DOVER STREET SB	1			1			
N095	EUSTON STATION	V10	CLOUDESLEY ROAD TO COBOURG STREET SB				1		1	1
N098	WARREN STREET TO EUSTON	V10	CLOUDESLEY ROAD TO COBOURG STREET SB				1		1	1
N098	WARREN STREET TO EUSTON	V08	COBOURG STREET TO DOVER STREET SB	1			1			
N101	WARREN STREET STATION	V08	COBOURG STREET TO DOVER STREET SB	1			1			
P065	GREEN PARK STATION	V06	DOVER STREET TO GILLINGHAM STREET SB				6 1			
V042	OXFORD CIRCUS TO WARREN STREET	V08	COBOURG STREET TO DOVER STREET SB	1			1 1	1	1	
V044	GREEN PARK TO OXFORD CIRCUS	V08	COBOURG STREET TO DOVER STREET SB	1			1 1	1	1	
V044	GREEN PARK TO OXFORD CIRCUS	V06	DOVER STREET TO GILLINGHAM STREET SB				6 1 1	1	1	
V046	VICTORIA TO GREEN PARK	V06	DOVER STREET TO GILLINGHAM STREET SB				6 1 1	1	1	
V047	VICTORIA STATION	V06	DOVER STREET TO GILLINGHAM STREET SB		1	1	6 1 1	1	1	
V047	PIMLICO TO VICTORIA	V06	DOVER STREET TO GILLINGHAM STREET SB		1	1	6 1 1	1	1	
V052	PIMLICO TO VICTORIA	V04	GILLINGHAM STREET TO STOCKWELL SB		1	1	4 1 1	1	1	

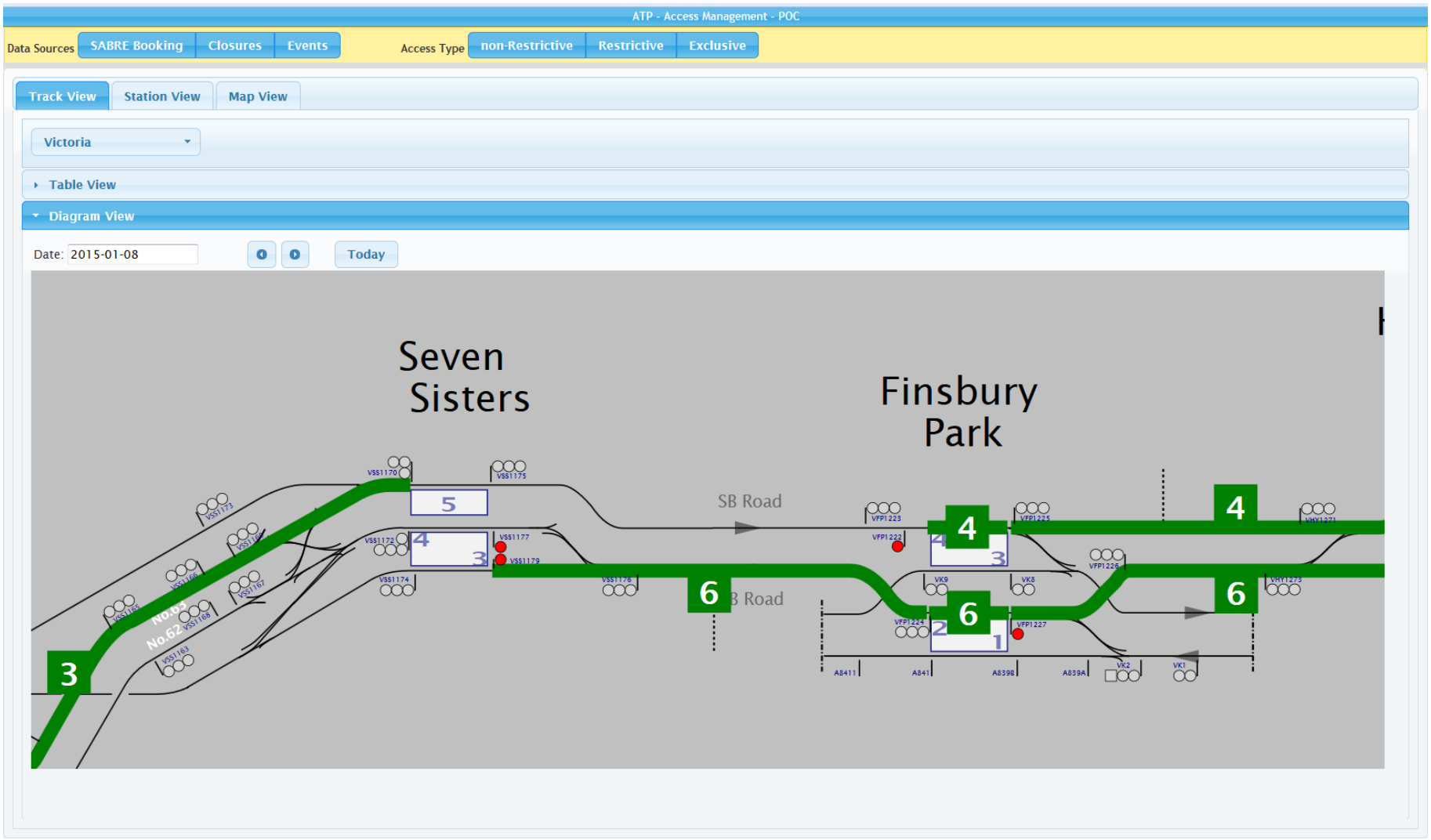


BTS Description	Accountable Manager	Request Set Status	Accountable Manager Phone Number	Track General Location	BTS Shift Date	Category of Work	Description of Work	Sabre Number	TCS Code	TCS Description	Track Booking Type	Track Purpose of Access	Track Status	Track Work Methods
5142 points - Victoria platform south end	DAVE JONES	Approved	0791 910 8673	Victoria platform Grounds + 200M (VICTORIA LINE)	2015-08-01	Upgrade/Renewals /Project	Install, survey and maintain structural monitoring equipment. Nova Victoria (formerly Victoria Circle) project. OANS: 1906,0979,2209.	2334027	V05	GILLINGHAM STREET TO DOVER STREET NB	Non-Exclusive / Non-Restrictive	Test equipment	Approved	Hand Tools
5142 points - Victoria platform south end	GARRY BURKE	Approved	02077877401	GREEN PARK TO PIMLICO ALL	2015-08-01	Upgrade/Renewals /Project	VICTORIA STATION RADIO/FIBRE INSTALLATION. TESTING & CUTOVERS	2335135	V05	GILLINGHAM STREET TO DOVER STREET NB	Non-Exclusive / Non-Restrictive	Comms	Approved	Other
5142 points - Victoria platform south end	M LEWIS	Completed	01189 699 777	VICTORIA PLATFORMS 3 & 4 TO SUB GAP - TO INCLUDE ROADS 22 & 23	2015-08-01	Upgrade/Renewals /Project	VICTORIA LINE - VICTORIA ATMS PROJECT	2333974	V05	GILLINGHAM STREET TO DOVER STREET NB	Non-Exclusive / Non-Restrictive	Comms	Completed	Hand Tools
5143 points - Victoria Siding 22 rd south end	Tony Vigor	Approved	02079183131	Victoria No 22 Siding, S.B (EH COT-SOT)	2015-08-01	Other	---STABLING--- Trains Stabled in accordance with Victoria WTT 36 effective 22/06/14 Locations covered: Victoria	2333561	V06	DOVER STREET TO GILLINGHAM STREET SB	Restrictive	Other	Approved	Outstable train
Green Park platform north end - Green Park platform south end	Ann Cumming	Completed	02079606803	GREEN PARK - BOTH.	2015-08-01	Maintenance/Servicing	INSTALLATION & REMOVAL OF TRACKSIDE POSTING AND PLACEMENT OF STRIPPING BAGS. MAINTENANCE OF LAMPS AND CLEANING OF XTP (PROJECTOR) EQUIPMENT ON PLATFORMS	2334829	V06	DOVER STREET TO GILLINGHAM STREET SB	Non-Exclusive / Non-Restrictive	Premises '&' structures	Completed	Renew
Green Park platform	Mark Fuller	Approved	07774 861713	Green Park Platform 3	2015-08-01	Installation/Removal	Installation of advertising signage in cross	2333987	V06	DOVER STREET	Non-Exclusive /	Signage	Approved	Hand Tools

F2.2 Diagram View

The track diagram view is a track line diagram based view of the underground showing key assets used in the access planning process (signals, points, platforms, stations and TCS). The user is able to select a specific day and then zoom in or out of the diagram to see the relevant details of potential bookings. There is a feature to be able to look at next and previous days data. This enables the user to keep the same level of zoom and geographic location and view the bookings for different days. Just like other views this is very useful to see gaps and bookings on the area of track in question. The track bookings are shown as lines over the sections the booking refer to. Where multiple bookings exist there is a count shown. The user is able to select the booking(s) and view the details of the booking in a grid.

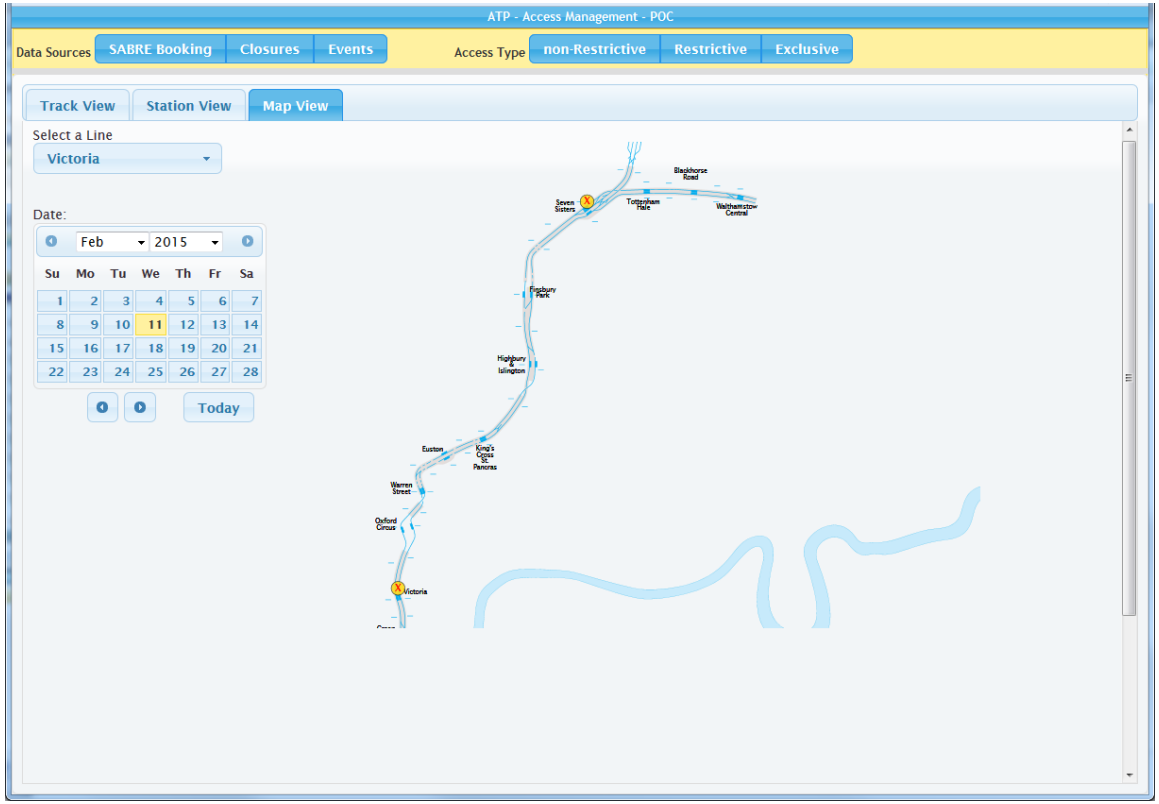

ATP - Access Management - POC
Data Sources
SABRE Booking
Closures
Events
Access Type
non-Restrictive
Restrictive
Exclusive
Track View
Station View
Map View
Victoria
Table View
Diagram View
Date: 2015-01-08
Today
Walthamstow Central
Blackhorse Road
Tottenham Hale
Seven Sisters
Finsbury Park
Highbury & Islington
King's Cross St. Pancras
Euston
Warren Street
Oxford Circus
Green Park
Victoria
Pimlico
Vauxhall
Stockwell
Brixton


ATP - Access Management - POC
Data Sources
SABRE Booking
Closures
Events
Access Type
non-Restrictive
Restrictive
Exclusive
Track View
Station View
Map View
Victoria
Table View
Diagram View
Date: 2015-01-08
Today
Seven Sisters
Finsbury Park
SB Road
B Road
No.62
3
5
4
6
VSS1170
VSS1175
VSS1177
VSS1179
VSS1172
VSS1176
VSS1174
VFP1223
VFP1222
VFP1225
VFP1226
VFP1224
VFP1227
VK9
VK8
VK2
VK1
A8411
A841
A839B
A839A

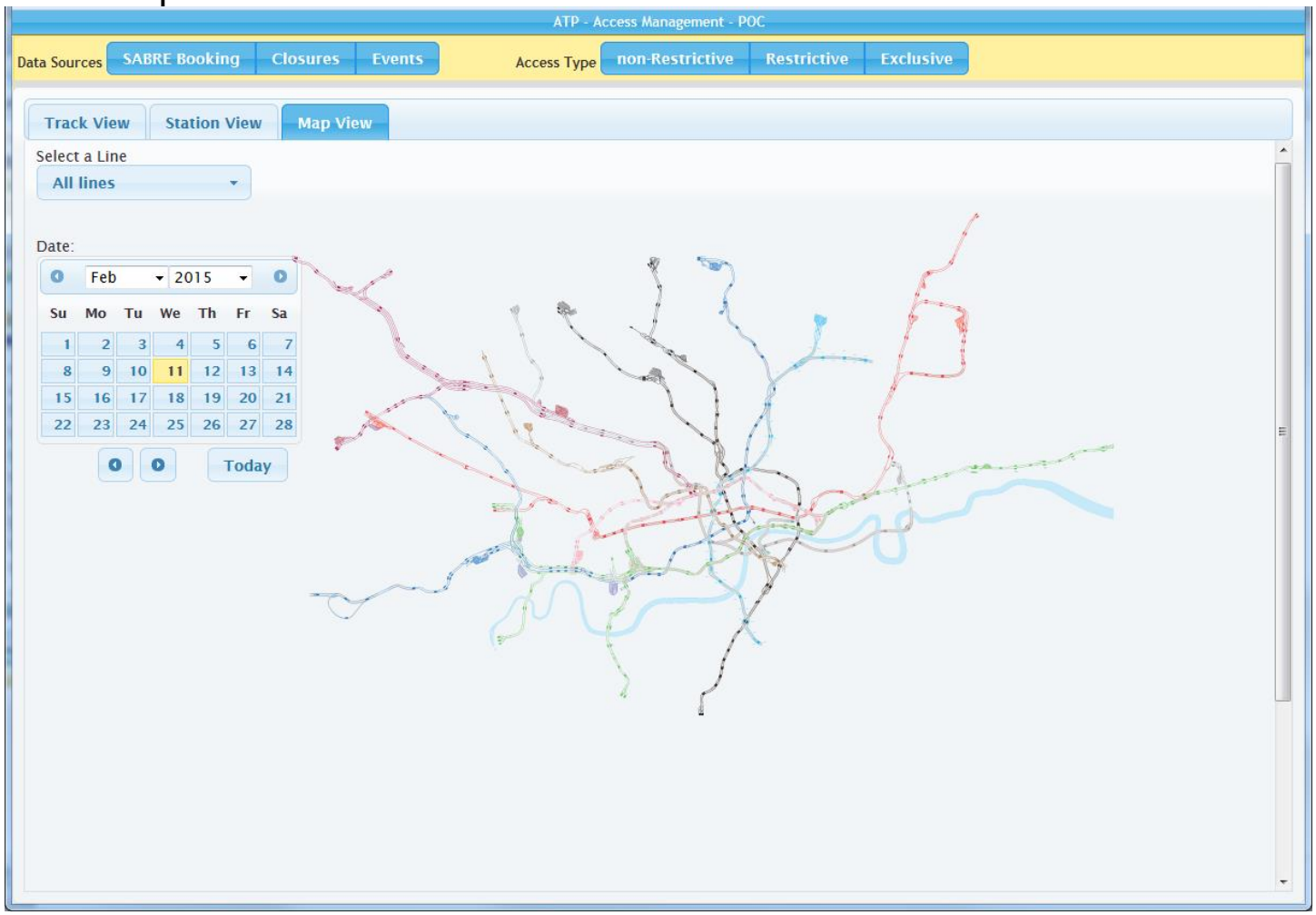
F3 Map View

A map based view of the underground network is more applicable for viewing events and closures information than access bookings. Included below are two examples of maps that could be useful.

F3.1 Line Map

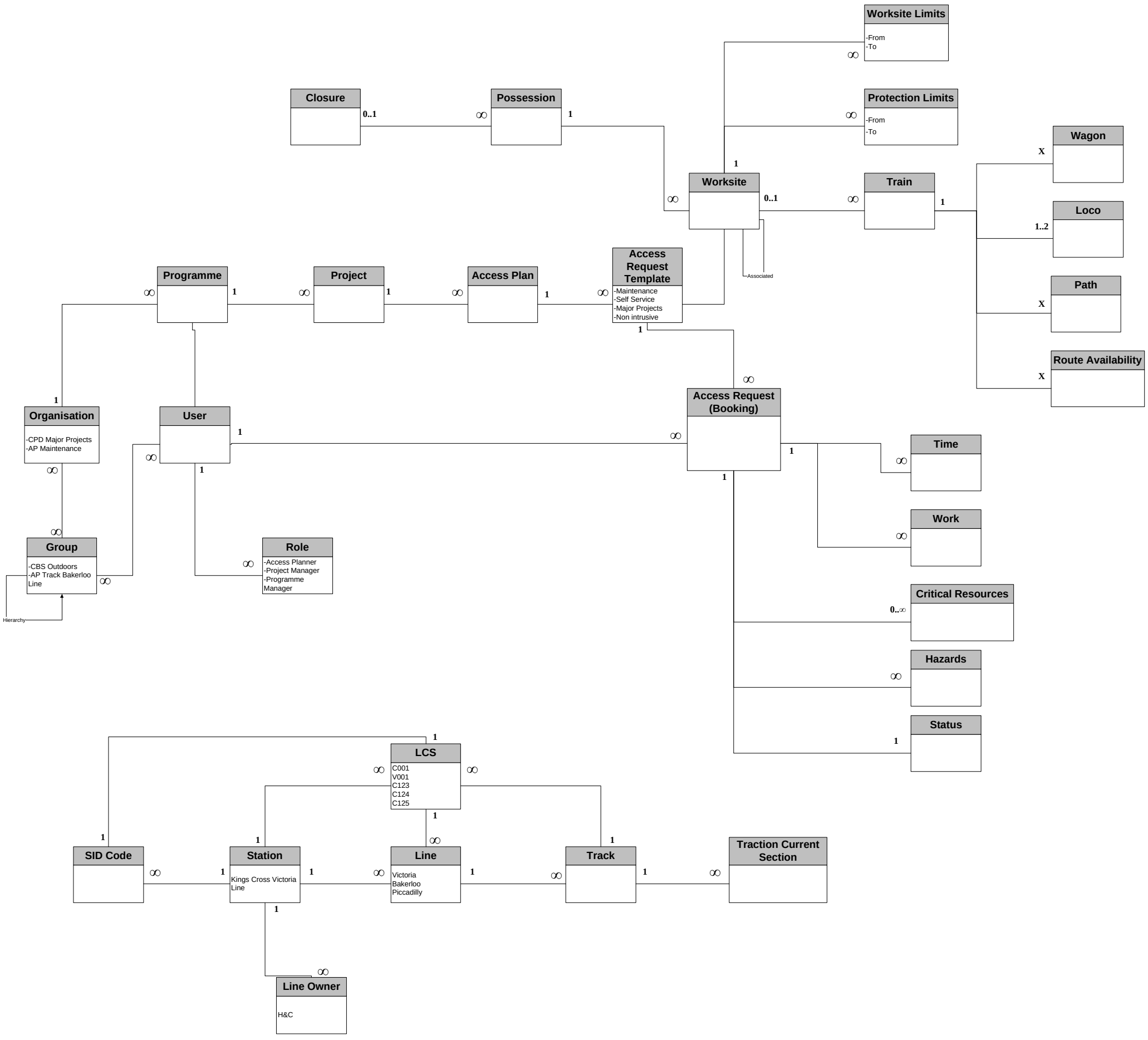


F3.2 Network Map



Appendix G: Access Planning Class Diagram

The following diagram shows the relationship between the main data types and attributes of the Access Planning System. This diagram is not a complete reflection of all of the data types only the key types required for access planning. This diagram should give a clear picture of how data items in the new system might be related.



Appendix H: Examples Access Planning System Business Rules

The table below list a number of example business rules that could be included within the Access Planning System.

Example No.	Business Rule Category	Business Rule Name	Business Rule Description
1	Access Request Classification	Access Type Classification	This business rule determines the access type of a booking. The access types are: • Exclusive • Restrictive • Non Exclusive/Non Restrictive See Ref-050 Appendix L for a definition of the existing Access Portal Business Rule that describes the Access Type.
2	Access Request Classification	Urgency Rule	This business rule defines the current lead times for access booking requests. The lead time is based on the combinations of selection criteria for the booking. See Ref-050 Appendix L for a definition of the existing Access Portal Business Rule that describes the Urgency.
3	Access Request Workflow	Self Serve – Not considered for planning	Work request is approved upon submission unless the worksite overlaps an existing Exclusive or restrictive worksite. The user will be notified if, subsequently to the submission, a new Exclusive or Restrictive worksite is approved that impinges on their worksite. If this occurs the requester will need to re-plan their worksite or contact the Access team for advice.
4	Access Request Workflow	Self Serve – Considered for planning	Work request is approved upon submission unless the worksite overlaps an existing Exclusive or restrictive worksite. The user will be notified if, subsequently to the submission, a new Exclusive or Restrictive worksite is approved that impinges on their worksite. If this occurs the requester will need to re-plan their worksite or contact the Access team for advice. Work requests of this type will show up in all reports used by the Access Planning team to consider when planning works in the same time/location.
5	Access Request Workflow	Maintenance	The maintenance access booking is either imported from a cyclical maintenance plan or created from a maintenance work booking template. Work requests of this type will show up in all reports used by the Access Planning team to consider when planning works in the same time/location.
6	Access Request Workflow	Requires Planning	Work requests are allocated to the relevant access planning teams for further refinement and approval. A possession and or closures workflow may be initiated.
7	Access Request Workflow	Possession	A possession work flow requires a possession plan to be created. The other opportunities for work are considered. The possession plan is verified and published at a defined number of weeks before the possession start date. Last minute changes are verified and published a defined number of days before the possession start date.
8	Access Request Workflow	Closure	The closures workflow requires approval and further refinement form the TfL S&SD department. The system will integrate with S&SDs closures planning database to achieve this.

9	Access Request Workflow	Staff Resourcing Requirements	Where a work request, a possession plan, a train request requires specific resources this is highlighted to the resource booking desk a defined number of days prior to the date that the resource is required. The resource booking desk can indicate that all resources required have been allocated to named individuals.
10	Access Request Workflow	Train Resourcing Requirements	Where a work request, a possession plan requires specific train resources this is highlighted to the train booking desk a defined number of days prior to the date that the train is required. The train booking desk can indicate that all trains required have been booked, have associated load plan and any staffing requirements fulfilled (train operation crew and loading plan are the responsibility of train operator).
11	Lock down Workflow	Lockdown of access requests	All work requests that require planning intervention must be received a defined number of weeks prior to the work start date. This number varies on the request type as per the access charter. The overall access plan for a single shift is verified and locked against further changes a defined number of hours before the shift commences. Additional approval is required from the access manager for all requests or changes that fall out of these timescales.
12	Train Consist Rules	Train Consist	Engineering Train Consist and Formation Rules The train and its constituent parts must be approved on LU infrastructure. A train must have compatible locos either end. Some wagons can only couple with other specified wagons Some Locos can only couple with other specified wagons Total train length cannot be greater than a specified length
13	Train Pathing Rules	Train Pathing	The train and its constituent parts can only travel on lines that they have been approved for. The train may have to be the last train i.e. no trains can pass over the route until the start of traffic after it has run. The train and its load must fit in the load gauge of the route. The train may have to be the only train operating on the line (or section of the line) and therefore must run in a possession. See Appendix L Ref-020.

14	Possessions Workflow	Possessions Workflow	 EIC – Engineer In Charge PWG – Possessions Works Guide PPLN – Possessions PLaN TO's – Technical Officer MCP – Manager In Change of Possessions ODM – Operations Duty Manager EH – Engineering Hours

Appendix I: Information Required for Access Planning

The matrix below shows the base information required to be available within the Access Planning System for users to successfully perform their role. Not all information is mandatory within the Planning System available however understanding the whole information requirements will help design the solution. Some of the information maybe better delivered to the users by other more appropriate systems outside of the Access Planning System such as GIS. Information that must be visible within the Access Mandatory information is shown as Y and optional information is shown as O. Not all of the users of the system would choose to use or see all of the information. E.g. Station planners would not be required to understand the train route availability and Train Path Planners would not be required to know detailed information around stations.

Example source Of Information	Reference	Information	Optional/Mandatory
Access Planning Visualisations	Appendix F	Track Layout - Geographic	Y
Access Planning Visualisations	Appendix F	Track Layout - Harry beck	Y
Access Planning Visualisations	Appendix F	Track Layout diagram	Y
Axonometric Station Diagrams	Appendix L Ref-024, Ref-025, Ref-026	Station Layout	Y
		Gradients	Y
		Curvature	O
Traffic Circular		Speed Restrictions	Y
Traffic Circular		Temporary Speed Restrictions	Y
		Track distances	Y
		Platform lengths	Y
		Siding Lengths	Y
		Junction lengths	Y
Harry Beck Map with LCS Codes	Appendix L Ref-021	LCS (Location Coding Structure)	Y
		Traction Current Isolation Switches	Y

		Traction Current Change Over Switches	Y
Traffic Controller Diagrams	Appendix L Ref-055	Signal Overlap	Y
Traffic Controller Diagrams	Appendix L Ref-055	Signals, Headway Post	Y
		Access Points Post Codes	O
Traffic Controller Diagrams	Appendix L Ref-055	Types of Points (Trailing or facing etc)	Y
		Track Circuits	O
Infrastructure Line Overview	Appendix L Ref-023	Cable Bridges	Y
Infrastructure Line Overview	Appendix L Ref-023	Staff Bridges	Y
Infrastructure Line Overview	Appendix L Ref-023	Twin Bore	Y
Infrastructure Line Overview	Appendix L Ref-023	Single Bore	Y
Infrastructure Line Overview	Appendix L Ref-023	Cut and Cover	Y
Infrastructure Line Overview	Appendix L Ref-023	Outside Section	Y
Infrastructure Line Overview	Appendix L Ref-023	Power Sub Gap	Y
Infrastructure Line Overview	Appendix L Ref-023	Trap Points	Y
Infrastructure Line Overview	Appendix L Ref-023	Unelectrified Trap Sidings	Y
Infrastructure Line Overview	Appendix L Ref-023	Unelectrified Track	Y
Infrastructure Line Overview	Appendix L Ref-023	Electrified Trap Sidings	Y

Infrastructure Line Overview	Appendix L Ref-023	Continuously Alive Track	Y
Infrastructure Line Overview	Appendix L Ref-023	Sub Gap < 60m from Platform	Y
Infrastructure Line Overview	Appendix L Ref-023	Line Clear Areas	Y
Infrastructure Line Overview	Appendix L Ref-023	Points	Y
Infrastructure Line Overview	Appendix L Ref-023	Platform Configuration	Y
Infrastructure Line Overview	Appendix L Ref-023	Station Name	Y
Infrastructure Line Overview	Appendix L Ref-023	Station Management Group	Y
Infrastructure Line Overview	Appendix L Ref-023	Train Operations Management Group	Y
Infrastructure Line Overview	Appendix L Ref-023	LCS Station	Y
Infrastructure Line Overview	Appendix L Ref-023	LCS Track (Interstation)	Y
Infrastructure Line Overview	Appendix L Ref-023	Under Bridge	Y
Infrastructure Line Overview	Appendix L Ref-023	Over Bridge	Y
Infrastructure Line Overview	Appendix L Ref-023	Access Personnel Gate Width <1.8m	Y
Infrastructure Line Overview	Appendix L Ref-023	Access Personnel Gate Width >1.8m	Y
Infrastructure Line Overview	Appendix L Ref-023	From One Side Overbridge, Small Plant (Non Personnel)	Y

Infrastructure Line Overview	Appendix L Ref-023	From Both Sides Overbridge, Small Plant (Non Personnel)	Y
Infrastructure Line Overview	Appendix L Ref-023	Access Via Gate Near Track, Small Plant and Personnel	Y
Infrastructure Line Overview	Appendix L Ref-023	Access Large Plant with Personnel	Y
Infrastructure Line Overview	Appendix L Ref-023	Draught Relief	Y
Infrastructure Line Overview	Appendix L Ref-023	Ventilation Fans	Y
Infrastructure Line Overview	Appendix L Ref-023	Evacuation Point	Y
Infrastructure Line Overview	Appendix L Ref-023	Intervention Point	Y
Traction Current Section Diagrams	Appendix Ref-028	Traction Current Sections	Y
CART Extract	Appendix L Ref-051	Stabled Trains	Y
		Network Rail Train Timetable shared/adjacent tracks (First and last train information)	O
CART Extract	Appendix L Ref-029	First Train	Y
CART Extract	Appendix L Ref-029	Last Train	Y
CART Extract	Appendix L Ref-030	TC Switching Times	Y
CART Extract	Appendix L Ref-052	Train Frequencies	Y
Pathing matrix from Timetables Dept	Appendix L Ref-031	Engineering Train Available Paths	Y
Engineering Train Route Availability Document	Appendix L Ref-019	Engineering Train Route Availability	Y

SABRE Extract	Appendix L Ref-052	Station Rooms - L&E Machine rooms - Station control room -Ticket office -Signalling Equipment rooms -Power switching rooms -Mess rooms -Cupboards/Storerooms -Retail -Toilets	Y
SABRE Extract	Appendix L Ref-052	Station Zones -Cross passageways -Passageways -Stairs -L&E -Disused areas -Ventilation shafts -Staff accommodation -Public/non Public Areas	Y
Axonometric Station Diagrams	Appendix L Ref-024, Ref-025, Ref-026	Escalator	Y
Axonometric Station Diagrams	Appendix L Ref-024, Ref-025, Ref-026	Lifts	Y

Appendix J: Access Planning System Visualisations and Uses

The table below list some of the key roles that will use the Access Planning System and shows the most appropriate visualisation that may be of use to the role for planning and booking access. Some examples of visualisations are shown in Appendix F.

Access Planning Role	Visualisation Type	Notes
Access Requester (Track Maintenance Planner)	Track View – Table (Gant) View Diagram View	Goal: To ensure that the scheduled maintenance work can be carried out successfully and is not affected by any major closures, possessions or other restricted work. Information of Interest: Visibility of closures, events or major works that could affect the work.
Access Requester (Stations Maintenance Planner)	Calendar View Stations Plan	Goal: To ensure that the scheduled maintenance work can be carried out successfully and is not affected by any major closures, possessions or other restricted work. Information of Interest: Visibility of closures, events or major works that could affect the work.
Access Requester (Non-intrusive Station Work)	Calendar View	Goal: To be able to successfully carryout some general access (usually less complex work) without other work in the station interfering. Problem: It is not easy to see other work that is taking place in a station and plan work around it. Much of the time this type of requester is flexible as to when and where they can work and so able to swap work to less busy times. Information of Interest: Visibility of station closures, events or station works that

		could affect my work. Only stations that they are interested in. Volumes of work by zone at a given station.
Access Requester (Escalator Maintainer)	Calendar View Stations Plan	Goal: To be able to carryout a maintenance activity on some escalator equipment in a machine room and ensure when planning the work it is coordinated when necessary with other work that is required to take place. Problem: Sometimes the work being carried out in a machine room is not easily done when sharing a space with other maintainers. This work could have been better coordinated or done on another night. Information of Interest: Visibility of work they could be going on in the same location that could make my work activity difficult to achieve.
Possessions Planner Track Access Planner	Track View – Table (Gant) View Diagram View	Goal: Access Planning team member requiring to plan multiple activities of different types into a very busy maintenance window. Problem: It is not always easy to see quickly when other work is planned . It is not always obvious when work can be successfully planned together. Information of Interest: Visibility of closures, events or other works that could affect the work to be booked or planned. Require visibility of the area of the network where the work is required and the full calendar of work over time. Depending of the maturity of the planning, work/tasks may need to be visible to the nearest hour rather than day. This can be achieved in the gant style visualisation. Non possessions type work may be required to be planned with the same level of granularity as possessions to gain more efficient use of access.

Stations Access Planner	Calendar View Stations Plan	Goal: Access Planning team member requiring to plan multiple activities of different types into a very busy maintenance window. Problem: It is not always easy to see quickly when other work is planned . It is not always obvious when work can be successfully planned together. Information of Interest: Visibility of closures, events or other works that could affect the work to be booked or planned. Require visibility of the station in question and the full calendar of work over time. Work by station zones.
Senior Manager/Director Role	Map view – Network Map View - Line	Goal: To be able to visualise totals of work categorised by work type and compare different station and track locations on the underground network. Problem: Not able to easily access network wide information on station and track access work. Information of Interest: Visibility of numbers of closures, events, major works and other work planned to carried out at stations and track (At station and interstation level of granularity)

Appendix K: Track Access Planning Aids/Reports

The following reports are used by the track access planners to help them with the track access planning.

Ref No. Appendix L	Report Name	Description
Ref-044	Train Plan	This report is used by the track planning team to help show all of the request for work that require engineering trains. The report is extracted from SABRE. The report is not a reflection of the train paths required to support the booking only the work sites that the train will work or be required in to support the booking. This report only have high level information on the requirement for the train and has no train consist or formation information.
Ref-045	TCS Lookahead	This report is a breakdown of the track bookings against the traction current sections for the line in question. This is shown a s a grid of bookings versus TCS. The contents of this report are only for exclusive and restrictive access bookings. The TC sections in which the train is required to work in to support the booking are shown. This spreadsheet is used to manage multiple bookings at the same location and date. The MS Excel filters help the user filter specific locations and timescales. If more than one booking can exist at the same time and location the status on the spreadsheet is set to approved. This information is taken directly from SABRE.
Ref-046	Graphical Representation of Bookings	This report is a more formal representation of the above TCS look ahead report. There is one report per underground line.

Ref-047	TWEAK Report	This report shows multiple booking of various status on a single report. The report brings together work requests from the access portal, SABRE bookings and train bookings on one single report. This report give visibility of up and coming work that is in draft state and aligns the potential and actual booking against TCS. The information in this report is only for a week of bookings.
Ref-048	Depot and Sidings Report	This report shown all of the bookings present in the depot or sidings.

Appendix L: Access Planning References

The documents listed are useful examples of existing documentation and drawings that can act as good background material to support the understanding of the access planning process. Some of the material is referred to in the requirements section of this document.

The location of this information is found in the included zip file called 'URS_RefFiles.zip'

Unique Ref No.	Type/Group	Title	Description	File Name and Location on Supplied Media
Ref-001	Publications	NEPA	Nightly Engineering Hours Protection Arrangements publication containing Last train information. Locations of engineer's trains and vehicles. Hazard areas. Traction current switching on and off times. This document is required for the staff providing protection.	URS_RefFiles\Publications\Publications Database\ NEPA_090115 (NEPA).pdf
Ref-002	Publications	Engineering Notice	The Engineering Notice for amendments of Engineer's trains and vehicles working on the railway. Possessions. Special current arrangements. Details of engineering works. Safety Issues. The audience for the document is Possession Master, Protection	URS_RefFiles\Publications\Publications Database\ 9_15 Fri (Eng Notice).pdf

			staff, Service Control, Power Control, Track Access Control, Planners, Transplant, APD, Upgrades.	
Ref-003	Publications	2 Week Look Ahead Engineering Notice	A 2 week look ahead of the Engineering Notice	URS_RefFiles\Publications\Publications Database\ enla-2-lookahead-v2 (EN 2 Week Look Ahead).pdf
Ref-004	Publications	PCRO NEPA	Power Control Room Operator (PCRO) version of the NEPA.	URS_RefFiles\Publications\Publications Database\ PCRO 09 January pdf (PCRO NEPA).pdf
Ref-005	Publications	General Access SABRE Report	Business Object report of access of type General extracted from the SABRE system for both track and stations work for a given time span.	URS_RefFiles\Publications\SABRE Publications\ General Access Plan 4642(General Access).pdf
Ref-006	Publications	Line Based Station Access Single Day SABRE Report	Business Object report of access of station access for the Victoria line, extracted from the SABRE system for a single day.	URS_RefFiles\Publications\SABRE Publications\ PWDailyVIC13_01_2015 (Vic Line Plan Works Daily).pdf
Ref-007	Publications	Line Based Station Access Weekly SABRE Report	Business Object report of access of station access for the Victoria line, extracted from the SABRE system for a week.	URS_RefFiles\Publications\SABRE Publications\ PWWeeklyVIC14_01_2015 (Vic Lined Plan Works Week).pdf
Ref-008	Publications	SABRE Station Access report for Exclusive and Restrictive Bookings	Business Object report of access of type Restrictive or Exclusive extracted from the SABRE system for stations work for a given time span.	URS_RefFiles\Publications\SABRE Publications\ SABN30 Res & Exc station Access 2767.xls

Ref-009	Publications	Possession Plan Report	Possessions publication created by the Possessions MS Access Database. All of the data contained within this report is entered into the database forms by possessions planners.	URS_RefFiles\Publications\Possessions Database\Possession Plan mock up.doc
Ref-010	Publications	Traditional Possessions Report	Possessions report create by manual methods by possessions planners.	URS_RefFiles\Publications\Possessions Database\PPLN-MET.JUB-NWD.RAL.WEP.STAtoCHC (FO2).pdf
Ref-011	Publications	Metropolitan Line Guide to Switching	Line based document showing TC switching times for all sections. Any amendments from previous versions are underlined.	URS_RefFiles\Publications\Guide to Switching\ Metropolitan line 11.11 wef 14 Dec (Guide to Switching).pdf
Ref-012	Publications	CLOSURE_SCHEDULE_201501131408 (Closures Schedule).xls	List of closures and detailed work within a closure over a given time period.	URS_RefFiles\Publications\Closures Database\ CLOSURE_SCHEDULE_201501131408 (Closures Schedule).xls
Ref-013	Publications	STABLING_TIMETABLE_201501131417 (Stabling Matrix - OOS).xls	Matrix of passenger train stabling locations for a given underground line. This is required as aid to the possession and access planning and inform planner s of any potential stabling conflicts with work planned.	URS_RefFiles\Publications\Closures Database\ STABLING_TIMETABLE_201501131417 (Stabling Matrix - OOS).xls
Ref-	Publications	WARM_20150113	Table of all of the closures and their corresponding work for a given time period,	URS_RefFiles\Publications\Closures Database\ WARM_20150113 (Weekly Action

014		(Weekly Action Review)	This is used in the existing process by the possessions planners as a starting point for the possession plan. This report contains the engineering trains required to support the work.	Review).xls
Ref-015	Publications	Depot Works Plan	Depot calendar based views of all work planned to take place at a depot over a period of time.	URS_RefFiles\Publications\Depot Works Plans\ DWP Hainault - Loughton - Woodford 08-05-12.xls DWP Neasden.xls DWP Northumberland Park Depot.xls DWP Ruislip Depot.xls DWP White City Sidings.xls
Ref-016	Forms	Access Plan	The Access Plan is a supplementary component of a commercial / contractual document which outlines the access provisions to be made for a specific commercial / contractual workstream.	URS_RefFiles\Forms\Access Plan Form\ F0259 ARF d2_4a.pdf
Ref-017	Forms	Access Request Form	An Access Request Form is made for a specific piece of work for which access I required, these will typically be made via the 'Access Portal', or alternatively may be made by email (usually for General	URS_RefFiles\Forms\Access Request Form\ F0259 ARF d1_3.xls

			Access).	
Ref-018	Trains	CTC - Certificate of Technical Conformance	Approval for Rolling Stock to be run on LU infrastructure.	URS_RefFiles\Trains\CTC - Certificate of Technical Conformance\ CTC 1269.pdf LU-CTC-648.pdf LU-CTC-1403.pdf
Ref-019	Trains	Permitted running routes for engineer's trains and heritage trains	In conjunction with the CTC this document specified the routes and train or stock can run on and any other limitations.	URS_RefFiles\Trains\Permitted Running Routes\ Permitted running routes for engineer's trains and heritage trains.pdf
Ref-020	Trains	Route Availability Certificate	Route Availability Certificate	URS_RefFiles\Trains\Route Availability Certificate\ WJM1319A speno RR24 MC_7.pdf
Ref-021	Maps and Diagrams	TCS Code Map	Harry Beck map of all underground stations with LCS codes included.	URS_RefFiles \Maps and Diagrams\LCS Maps\ LCScode Map#.pdf
Ref-022	Maps and Diagrams	Geographic Map	Geographic map of the underground showing depot and siding and major crossovers.	URS_RefFiles \Maps and Diagrams\LCS Maps\ Operations track overview (Lines & Junctions Geographical).pdf
Ref-023	Maps and Diagrams	Infrastructure Line Diagrams	Infrastructure Line overview diagrams (ILO) show the following information: -Track access points in line safe areas	URS_RefFiles \Maps and Diagrams\Infrastructure Line Diagrams\ Piccadilly ILO Diagram1 v2.1.pdf

			-Open and tunnel sections -Power supply points -Platform and tunnel configurations -LCS codes -Evacuation points -Ventilation fans	Piccadilly ILO Diagram2 v2.0.pdf Piccadilly ILO Diagram3 v2.0,pdf Piccadilly ILO Key1 v2.0.pdf Piccadilly ILO Key2 v2.0.pdf Piccadilly ILO Key3 v2.0.pdf Victoria ILO Diagram1 v2.0.pdf Victoria ILO Key1 v2.0.pdf
Ref-024	Maps and Diagrams	Axonometric Station Diagram Euston	Axonometric station diagrams of a Traditional Complex Station – Euston showing key locations of an underground station.	URS_RefFiles\Maps and Diagrams\Station Diagrams\ Euston Plan.pdf
Ref-025	Maps and Diagrams	Axonometric Station Diagram North Greenwich	Axonometric station diagrams of a Box station – North Greenwich showing key locations of an underground station.	URS_RefFiles\Maps and Diagrams\Station Diagrams\ North Greenwich Plan.pdf
Ref-026	Maps and Diagrams	Axonometric Station Diagram West Finchley	Axonometric station diagrams of a simple Station – West Finchley showing key locations of an underground station.	URS_RefFiles\Maps and Diagrams\Station Diagrams\ West Finchley Plan.pdf
Ref-027	Maps and Diagrams	Track Access Control Maps	Track Access Control Maps showing traction current sections and phone numbers of track access desks	URS_RefFiles\Maps and Diagrams\Track Access Control Maps\

				Bloo_Issue13.pdf Cent_Issue15t.pdf …
Ref-028	Maps and Diagrams	Traction Current Section Diagrams	Traction Current Diagrams showing the locations of the different traction current areas	URS_RefFiles\Maps and Diagrams\Traction Current Section Diagrams\ Northern line V12 effective May 2013.pdf Victoria ILO Diagram1 v2.0.pdf
Ref-029	Timetable Files	Early and Late Current Files	Early and late current files extracted from CART for current sections that are switching at different times to the permanent timetable.	URS_RefFiles\Timetable Files\Early and Late Current Files\ EYCURRA050315.csv LTCURRA050315.csv
Ref-030	Timetable Files	Last Passenger Train	Last current file taken from iCART and produced in CART for all the last passenger trains for a given timetable.	URS_RefFiles\Timetable Files\ Last Passenger Train\ iCart
Ref-031	Timetable Files	Pathing Matrix Docs	List the spare paths within the timetable for engineering trains or other trains to be pathed to support track access work.	URS_RefFiles\Timetable Files\Pathing Matrix Docs\ District Matrix new run times.doc Northern Matrix new run times.doc
Ref-032	SABRE Documentation	SABRE Functional Requirements Document	One of the original requirements documents from the existing access	URS_RefFiles\ SABRE Documentation\ SABRE URS and FRS\ CR1\ FRS v 1.22.doc

			booking system SABRE. These document are not always a true reflection on the actual functionality within SABRE.	
Ref-033	SABRE Documentation	SABRE User Requirements Document	One of the original requirements documents from the existing access booking system SABRE. These document are not always a true reflection on the actual functionality within SABRE.	URS_RefFiles\ SABRE Documentation\ SABRE URS and FRS\ CR1\User Requirements Specification - SABRE Replacement v2.0.doc
Ref-034	SABRE Documentation	SABRE User Guide for Access Coordinators	SABRE User Guide for Access Coordinators	URS_RefFiles\ SABRE Documentation\ SABRE User Guides\ sabre-netuserguide-accesscoordinators.pdf
Ref-035	SABRE Documentation	SABRE User Guide for Access Admin	SABRE User Guide for Access Admin	URS_RefFiles\ SABRE Documentation\ SABRE User Guides\ sabre-netuserguide-administration.pdf
Ref-036	SABRE Documentation	SABRE User Guide for Managing Users	SABRE User Guide for Managing Users	URS_RefFiles\ SABRE Documentation\ SABRE User Guides\ sabre-netuserguide-managingusers.pdf
Ref-037	SABRE Documentation	SABRE User Guide for Access Planners	SABRE User Guide for Access Planners	URS_RefFiles\ SABRE Documentation\ SABRE User Guides\ sabre-netuserguide-planners.pdf
Ref-038	Closures	Closures Extract	Closures Extract from the Events & Closures Database.	URS_RefFiles\Closures\Closures Example from Closures DB.xlsx

Ref-039	Events	Events Extract	Events Extract from the Events & Closures Database. An event will affect many sections of line and so the affected location are included in the second spreadsheet.	URS_RefFiles\Ecents\ Events Example.xlsx Events including Affected LCSs .xlsx
Ref-040	Maintenance Schedules	Maintenance Schedules	Some of the repetitive maintenance schedules for the underground network. These files are produced by the asset maintenance teams within London Underground and sent to the access department.	URS_RefFiles\ Maintenance Schedules\ B&V_48_week_Master_Schedule_.xlsx Central_Master_Schedule_48_week.xlsx SSL_North_48_week_Master_Schedule_.xlsx
Ref-041	Possessions Planning	Possessions Diagrams	The diagrams used by the possession planners to plan the possessions work. The same diagram is issued as part of the possession report.	URS_RefFiles\Planning\ Possession Diagrams\Possession Worksite Information Diagrams.doc
Ref-042	Possessions Planning	Possessions Planner Database User Guide	Possessions Planner Database User Guide	URS_RefFiles\Planning\Possession Planner Database User Guide.pdf
Ref-043	Station Planning	Stations OAN	Station OAN (Operational Acceptance Notice) is used to ensure that the work due to be carried out on the station is suitable and agreed by the station landlord. All of this document is information previously captured in either the access plan or access request.	URS_RefFiles\Planning\Station OAN\ 0205 E-OAN Oxford Circus.pdf 0210 E-OAN Gunnersbury.pdf 0238 E-OAN King's Cross.pdf 0283 E-OAN Holborn.pdf

				0294 E-OAN Piccadilly Circus.pdf OAN Template v1.3 June 2014.docx
Ref-044	Track Planning	Train Plan	This report is used by the track planning team to help show all of the request for work that require engineering trains	URS_RefFiles\Planning\Track Planning Reports\SSL EHACM Data (Trains).xls
Ref-045	Track Planning	TCS Lookahead	This report is a breakdown of the track bookings against the traction current sections for the line in question.	URS_RefFiles\Planning\Track Planning Reports\TCS Lookahead.xls
Ref-046	Track Planning	Graphical Representation of Bookings	This report is a more formal representation of the above TCS look ahead report. There is one report per underground line.	URS_RefFiles\Planning\ Published VIC.pdf
Ref-047	Track Planning	TWEAK Report	This report shows multiple booking of various status on a single report	URS_RefFiles\Planning\ TWEAK Data Sheet wc20th Apr 2015.xls
Ref-048	Track Planning	Depot and Sidings Report	This report shown all of the bookings present in the depot or sidings.	URS_RefFiles\Planning\ Depot Planning Report.xls
Ref-049	Forms	Access Request Portal Fields	Access Request Portal Field List	URS_RefFiles\Forms\Access Request Portal Fields.xls
Ref-050	Planning	Access Request Portal Business Rules	The business rules implemented in the existing access request portal to deliver the Urgency Rule and Allocated to Rules (Access Type).	URS_RefFiles\Planning\Access Request Portal Business Rules.xls

Ref-051	Timetable	Stabled Trains	This is an extract from the CART system showing the stabled trains .	URS_RefFiles\Timetable Files\Stabled Trains\ TIMETABLE_STABLING_DATA.xlsx
Ref-052	Timetable	Train Frequencies	This file is a summary of the number of trains per hour for the Central line. This file is a cleaned up extract from the CART system.	URS_RefFiles\Timetable Files\Central WTT67 2015 September 2013.pdf
Ref-052	SABRE	SID Codes and Zones	Example list of station room codes (SID Codes) and corresponding station zones.	URS_RefFiles\ SABRE Documentation\ SID Codes and Zones.xlsx
Ref-053	Access Request Examples	Access Request Examples	Access Request examples taken from either the access request portal or the ARF forms. Both sources contain similar information.	URS_RefFiles\ Request and Booking Examples\ 2344455 Seven Sisters E3 09 Feb to 09 March 2015.xls ARF Mar 2015 track.xls AQ00003680.pdf AQ00004333.pdf APDBCVS12wk1.pdf APDBCVS16wk9.pdf APDSSL12wk1.pdf APDSSL16wk9a.pdf

Ref-054	Access Booking Examples	Access Booking Examples	SABRE Booking examples.	URS_RefFiles\ Request and Booking Examples\ 2346421.pdf 2345987.pdf 2345084.pdf 2344161.pdf 2344455.pdf 2346382.pdf 2346347.pdf 2345594.pdf
Ref-055	Maps and Diagrams	Traffic Controller Diagrams	The Traffic Controller's Diagrams (TCDs) provide vital information in the form of a layout plan showing two information sets. The upper part of the TCD displays a layout plan of the signalling arrangements and the lower part shows the sectionalisation and switching arrangements of the traction current. Both parts reflect the same area of the network.	URS_RefFiles\Maps and Diagrams\Traffic Controller Diagrams\ TS18888.pdf TS25076.pdf HS.111083 01 to 09 - Vic Line SCC TSR Areas.pdf AE30-TS-110777.pdf

Ref-056	Trains	Transplant Engineering Fleet Catalogue.	Transplant Engineering Fleet Catalogue.	URS_RefFiles\Trains\ Transplant Engineering Fleet Catalogue.pdf
Ref-057	Forms	Access Request Template Example	Access Request Template Example	URS_RefFiles\Forms\Booking request template Example.doc
Ref-058	Traction Current	Traction Current Example File	Traction Current Example File	URS_RefFiles\Traction Current\Traction Current Section details – Example.xls
Ref-059	Forms	Application to Work Form	Application to Work Form currently used to request to work within a possession.	URS_RefFiles\Forms\Week 2 Ealing Common Depot TDU AWF.pdf
Ref-060	Possessions Planning	Scotch and Clip Types for Points across the network	Scotch and Clip Types for Points across the network	URS_RefFiles\Planning\Scotch and Clip Types.xls

Appendix M: Examples of Access Request for Different Types of Planning

The table below list a number of example work requests that relate to the different access planning types defined in Appendix B with the associated SABRE booking number. This table enables an understanding of how an originating access request is delivered as a track or station booking within the Access department under the existing process. All of the examples can be found in Appendix L Ref-053 and Ref-054.

No.	Access Planning Type	Planning Type ID	Access Planning Request Reference (Taken from the Access Request Portal or other source)	Corresponding SABRE booking Number (taken from the SABRE System)
1	Simple Track booking	**1a**		2347049.pdf
2	Simple Station Booking	**1b**	AQ00004333.pdf	2346421.pdf
3	Simple Track & Station Booking	**1c**	ARF Mar 2015 track.xls	2345987.pdf
4	Restrictive Track Booking	**2a**	AQ00004414.pdf	2347049.pdf
5	Restrictive Station Booking	**2b**		2345084.pdf
6	Exclusive Track Booking	**2e**	AQ00004019.pdf	2345740.pdf

7	Exclusive Station Booking	**2f**	AQ00003680.pdf	2344161.pdf
8	Station Closure (Major)	**3bi**	Tufnel Park, All lifts taken out for maintenance therefore major station closure	
9	Station Closure (L&E)	**3bii**	2344455 Seven Sisters E3 09 Feb to 09 March 2015..xls	2344455.pdf
10	Station Closure (Minor)	**3biii**	2344455 Seven Sisters E3 09 Feb to 09 March 2015.xls	2344455.pdf
11	Engineering Hours Possession	**4**	AQ00004232.pdf	2345992.pdf
12	Track Eng Hours Possession With Train	**6**	AQ00003850.pdf AQ00005049.pdf	2346606.pdf
13	Cancel Engineering Hours With Trains Cancel Engineering Hours	**12**	AQ00004463.pdf	2347041.pdf
14	Maintenance Work	**13**	APDBCVS12wk1.pdf APDBCVS16wk9.pdf APDSSL16wk9a.pdf	2346382.pdf 2346347.pdf 2345594.pdf

Appendix N: Protection Resource Types Used within Planning Process

The table below shows the existing protection resource types contained within the OGMS system.

Resource_Type_Code	Resource_Type	Resource_Company
ASP	Assistant Possession Master	London Underground
BANCE	BANCE	London Underground
TM-TBTC-V	Certified Train Master	London Underground
ASS	D32 Assessor	London Underground
DEICE-SPC	De-Icer SPC	London Underground
DEICE	De-Icing	London Underground
EIC	Engineer In Charge	London Underground
FWM	Fire Watchman	London Underground
LSPC	Lead Site Person in Charge	London Underground
LKT	Lookout	London Underground
NSC	Non Safety Critical Activities	London Underground
PSF	Possession Foreman	London Underground
PSD	Possession Master Depot	London Underground
PSM	Possession Master Main	London Underground
PST	Possession Master Train Movements	London Underground
POSUM	Possession Support Manager	London Underground
PRFR	Protection Foreman	London Underground
PRME	Protection Master - Engineering Hours	London Underground
PRMT	Protection Master - Traffic Hours	London Underground

PDC	Protection Master Dual Certified	London Underground
PDCS	Protection Master Dual Certified/SPC	London Underground
PMSE	Protection Master Engineering Hours/SPC	London Underground
PMST	Protection Master Traffic Hours/SPC	London Underground
PMS-TL	Protection Master/SPC-Team Leader	London Underground
SAC	Site Access Controller	London Underground
TNR	Train Master	London Underground
TRAIN_SPC	Train SPC	London Underground
WORKSITE	Worksite Cordination Grades	London Underground
COSS	Network Rail Controller of Site Safety	Network Rail
NRCC	Network Rail Crane Controller	Network Rail
NRCC-TL	Network Rail Crane Controller - Tandem Lifter	Network Rail
NRCC-F	Network Rail Crane Controller Foreman	Network Rail
NES	Network Rail Engineering Supervisor	Network Rail
NRHS	Network Rail Hand Siganller	Network Rail
NRHBK	Network Rail Handback	Network Rail
NLKT	Network Rail Lookout	Network Rail
NRPO	Network Rail Points Operator	Network Rail
NRPC	Network Rail Protection Controller	Network Rail

NRSIM	Network Rail Site Manager	Network Rail
SW	Network Rail Site Warden	Network Rail
NWSTR	Network Rail Strapman	Network Rail
NWR-LCA	NWR - LEVEL CROSSING ATTENDANT	Network Rail
NWSTR-A	NWR Strapman Level A	Network Rail
PICOP	Network Rail PICOP	Network Rail
SPICOP	Network Rail SPICOP	Network Rail

Appendix O: TfL Geographic Information System (GIS)

LU GIS and Spatial Model

The Spatial Model

LU maintains a spatial model of the LU network to enable assets or events to be visualised in the GIS. The spatial model defines the LU property boundaries and captures the location of asset groups within these boundaries. These asset groups are:

- The Permanent Way – this is the track corridor, including depots and sidings, bounded by fencing and containing: Track, Civils, Signals, Power and Premises assets. .
- Stations – which include the main station building and other Premises within the property boundaries. The asset groups contained within stations are: Signals, C&I, Civils, L&E, Power, Mechanical, Electrical, Fire and Telecoms.
- High Voltage Power Distribution Network – these assets are remote from Stations and the Permanent Way and comprise of sub-stations and the HV cable distribution network. Some HV Power assets are also contained within the Permanent Way and Stations boundaries and in all cases have separate access arrangements.

The above asset groups comprise the assets that LU owns and manages and the spatial model enables the property boundaries and asset location to be defined to London Survey Grid.

The Geographical Information System

Using the spatial model the GIS enables assets or events to be viewed seamlessly against ordnance survey base mapping showing roads and buildings. The GIS also has aerial imagery and links to Bing and Google maps to further enhance the visualisation of the locations.

The GIS records all access points comprising of: access gates, bridges that allow craned access to the track, stations and vent shaft entrances. For stations, the GIS shows each room using Station Identification Codes that uniquely identifies each room. For the

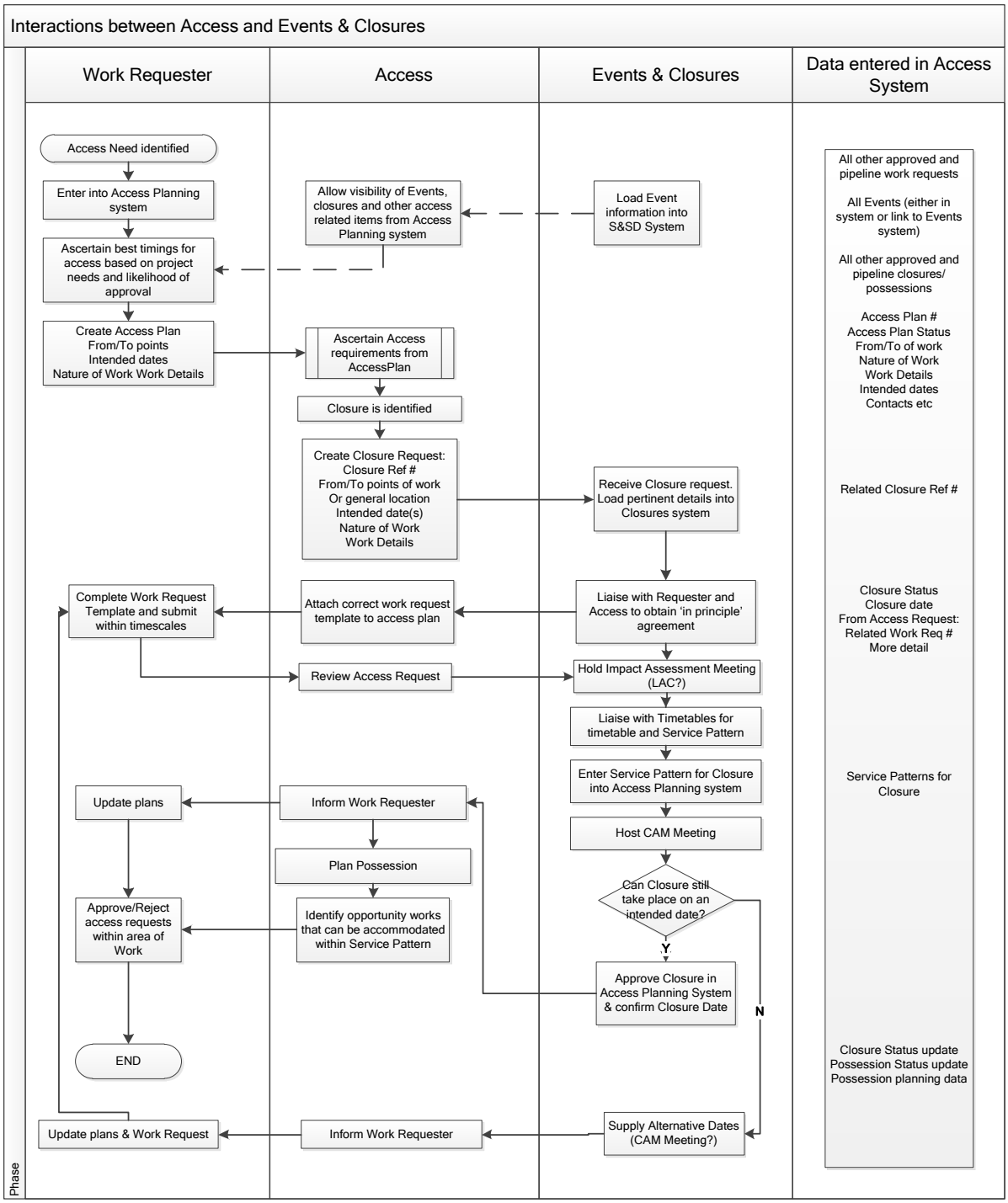
Permanent Way linear referencing is used to identify location as a track metreage or locations can be specified using GPS co-ordinates. Remote locations can be identified using street names and GPS co-ordinates.

The GIS is hosted on the TfL One London Network and is accessible on desktop and mobile devices and is also accessible to the supply chain using the Universal Access Gateway.

The GIS uses the Intergraph Geomedia 2014 Portal software that has 2D, 3D and 4D capability.

Appendix P: Closures Planning Process

The flow diagram below describes the process that is required to exist to manage the closures process within access planning.

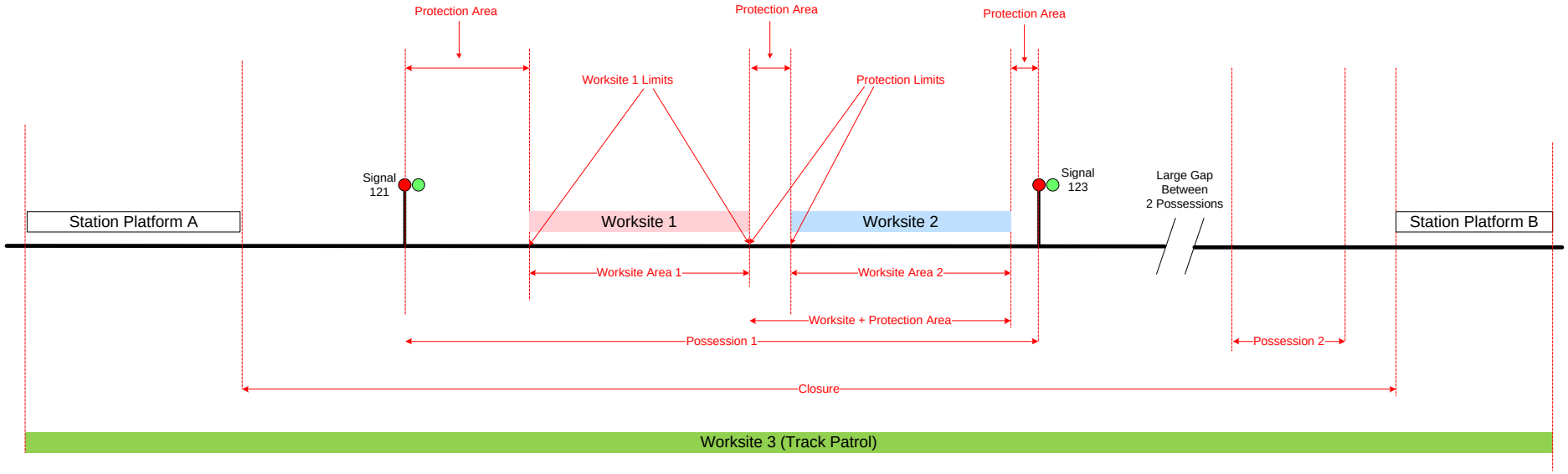


Appendix Q: Access Planning Limits Example

The diagram below is an example of how the following planning concepts interact and exist on the railway:

- Closure
- Possessions
- Worksites
- Worksite Protection Areas

Two possessions don't normally exist touching each other but exist as described in the diagram, separated by a significant geographic area. Both possessions can exist within the same Closure. A possession can exist without a closure when the possession is planned and operates in engineering hours and does not affect the operational railway. A possession can technically exist without worksites with it i.e. running a test train.



APPENDIX E

Access Planning URS Functional

TfL Access P

Tender Category	ID	Type	Phase	Function
External Customer Experience		**Heading**	**Data Capture**	**Define Programme**
External Customer Experience	001	Req	Data Capture	Define Programme
External Customer Experience	002	Req	Data Capture	Define Programme
External Customer Experience	003	Req	Data Capture	Define Programme
External Customer Experience	004	Req	Data Capture	Define Programme
Access Planning	315	Req	Data Capture	Assign Authorisation
External Customer Experience	005	Req	Data Capture	Define Programme
External Customer Experience	006	Req	Data Capture	Define Programme
External Customer Experience	007	Req	Data Capture	Define Programme
External Customer Experience	008	Req	Data Capture	Define Programme
External Customer Experience	009	Req	Data Capture	Define Programme

External Customer Experience		**Heading**	**Data Capture**	**Define Project**
External Customer Experience	010	Req	Data Capture	Define Project
External Customer Experience		**Heading**	**Data Capture**	**Create Access Plan**
External Customer Experience	011	Req	Data Capture	Create Access Plan
External Customer Experience	012	Req	Data Capture	Create Access Plan
External Customer Experience	013	Req	Data Capture	Create Access Plan
External Customer Experience	014	Req	Data Capture	Create Access Plan
External Customer Experience	015	Req	Data Capture	Create Access Plan
Access Planning		**Heading**	**Data Capture**	**Reviewing Access Plan**
Access Planning	017	Req	Data Capture	Reviewing Access Plan
Access Planning	018	Req	Data Capture	Reviewing Access Plan

Access Planning	019	Req	Data Capture	Reviewing Access Plan
Access Planning	020	Req	Data Capture	Reviewing Access Plan
External Customer Experience		**Heading**	**Data Capture**	**Create and Allocate Templates**
Access Planning	016	Req	Data Capture	Create and Allocate Templates
External Customer Experience	047	Req	Data Capture	Create and Allocate Templates
External Customer Experience	048	Req	Data Capture	Create and Allocate Templates
External Customer Experience	053	Req	Data Capture	Create and Allocate Templates
External Customer Experience	054	Req	Data Capture	Create and Allocate Templates
External Customer Experience	258	Req	Data Capture	Create and Allocate Templates
External Customer Experience	259	Req	Data Capture	Create and Allocate Templates
External Customer Experience	260	Req	Data Capture	Create and Allocate Templates
External Customer Experience	261	Req	Data Capture	Create and Allocate Templates
External Customer Experience	263	Req	Data Capture	Create and Allocate Templates
External Customer Experience	264	Req	Data Capture	Create and Allocate Templates
Access Planning		**Heading**	**Access Planning**	**Consider Closures**

Access Planning	027	Req	Access Planning	Consider Closures
Access Planning	028	Req	Access Planning	Consider Closures
Access Planning		**Heading**	**Access Planning**	**Consider Events**
Access Planning	023	Req	Access Planning	Consider Events
Access Planning	024	Req	Access Planning	Consider Events

Access Planning	025	Req	Access Planning	Consider Events
Access Planning	026	Req	Access Planning	Consider Events
Access Planning	029	Req	Access Planning	Consider Events
Access Planning	351	Req	Access Planning	Consider Events
Access Planning		**Heading**	**Access Planning**	**Consider Other Works**
Access Planning	030	Req	Access Planning	Consider Other Works
Access Planning	032	Req	Access Planning	Consider Other Works
External Customer Experience		**Heading**	**Access Planning**	**Create Track Booking**
External Customer Experience	056	Req	Access Planning	Create Track Booking
External Customer Experience	057	Req	Access Planning	Create Track Booking

External Customer Experience	058	Req	Access Planning	Create Track Booking
External Customer Experience		**Heading**	**Access Planning**	**Create Booking**
External Customer Experience	136	Req	Data Capture	Create Booking
External Customer Experience	137	Req	Access Planning	Create Booking
External Customer Experience	138	Req	Access Planning	Create Booking
External Customer Experience	139	Req	Access Planning	Create Booking
External Customer Experience	140	Req	Access Planning	Create Booking
External Customer Experience	141	Req	Access Planning	Create Booking
External Customer Experience	142	Req	Access Planning	Create Booking
External Customer Experience	143	Req	Access Planning	Create Booking
External Customer Experience	144	Req	Access Planning	Create Booking
External Customer Experience	145	Req	Access Planning	Create Booking
External Customer Experience	146	Req	Access Planning	Create Booking
External Customer Experience	147	Req	Access Planning	Create Booking
External Customer Experience	148	Req	Access Planning	Create Booking
External Customer Experience	149	Req	Access Planning	Create Booking
External Customer Experience	170	Req	Access Planning	Create Track Booking
External Customer Experience	268	Req	Access Planning	Create Track Booking
External Customer Experience	269	Req	Access Planning	Create Track Booking
External Customer Experience	270	Req	Access Planning	Create Track Booking
External Customer Experience	271	Req	Access Planning	Create Track Booking

External Customer Experience	350	Req	Data Capture	Create Booking
External Customer Experience	361	Req	Access Planning	Create Track Booking
External Customer Experience		**Heading**	**Access Planning**	**Create Station Booking**
External Customer Experience	265	Req	Access Planning	Create Station Booking
External Customer Experience	266	Req	Access Planning	Create Station Booking
External Customer Experience	267	Req	Access Planning	Create Station Booking
Access Planning		**Heading**	**Access Planning**	**Define Workflow and Approvals**
Access Planning	055	Req	Access Planning	Define Workflow and Approvals
Access Planning	199	Req	Data Capture	Define Workflow and Approvals
Access Planning	200	Req	Data Capture	Define Workflow and Approvals
Access Planning	201	Req	Data Capture	Define Workflow and Approvals
Access Planning	202	Req	Data Capture	Define Workflow and Approvals
Access Planning	203	Req	Data Capture	Define Workflow and Approvals
Access Planning		**Heading**	**Access Planning**	**Define Closure Limits and Scope**
Access Planning	033	Req	Access Planning	Define Closure Limits and Scope

Access Planning	034	Req	Access Planning	Define Closure Limits and Scope
Access Planning	035	Req	Access Planning	Define Closure Limits and Scope
Access Planning		**Heading**	**Access Planning**	**Agree Closure**
Access Planning	036	Req	Access Planning	Agree Closure

Access Planning	037	Req	Access Planning	Agree Closure
Access Planning	352	Req	Access Planning	
Access Planning		**Heading**	**Access Planning**	**Auto Approve Booking**
Access Planning	316	Req	Access Planning	Auto Approve Booking
Access Planning		**Heading**	**Access Planning**	**Load Maintenance Works/Create Bookings**
Access Planning	051	Req	Access Planning	Load Maintenance Works/Create Bookings
Access Planning	052	Req	Access Planning	Load Maintenance Works/Create Bookings
Access Planning	179	Req	Access Planning	Load Maintenance Works/Create Bookings
Access Planning	180	Req	Access Planning	Load Maintenance Works/Create Bookings
Access Planning		**Heading**	**Access Planning**	**Plan Worksite Limits**
Access Planning	078	Req	Access Planning	Plan Worksite Limits
Access Planning	279	Req	Access Planning	Plan Worksite Limits
Access Planning	280	Req	Access Planning	Plan Worksite Limits
Access Planning	281	Req	Access Planning	Plan Worksite Limits
Access Planning	049	Req	Access Planning	Other Planning
Access Planning	080	Req	Access Planning	Other Planning
Access Planning	081	Req	Access Planning	Other Planning
Access Planning	085	Req	Access Planning	Other Planning
Access Planning	086	Req	Access Planning	Other Planning

Access Planning	087	Req	Access Planning	Other Planning
Access Planning	089	Req	Access Planning	Other Planning
Access Planning	090	Req	Access Planning	Other Planning
Access Planning	113	Req	Access Planning	Other Planning
Access Planning	114	Req	Access Planning	Other Planning
Access Planning	115	Req	Access Planning	Other Planning
Access Planning	116	Req	Access Planning	Other Planning
Access Planning	117	Req	Access Planning	Other Planning
Access Planning	118	Req	Access Planning	Other Planning

Access Planning	119	Req	Access Planning	Other Planning
Access Planning	133	Req	Access Planning	Other Planning
Access Planning	134	Req	Access Planning	Other Planning
Access Planning	212	Req	Access Planning	Other Planning
Access Planning	213	Req	Access Planning	Other Planning
Access Planning	214	Req	Access Planning	Other Planning
Access Planning	319	Req	Access Planning	Other Planning
Access Planning	347	Req	Access Planning	Other Planning
Access Planning	353	Req	Access Planning	Other Planning
Access Planning		**Heading**	**Access Planning**	**Plan Protection Limits**
Access Planning	079	Req	Access Planning	Plan Protection Limits
Access Planning	282	Req	Access Planning	Plan Protection Limits
Access Planning	283	Req	Access Planning	Plan Protection Limits
Access Planning	284	Req	Access Planning	Plan Protection Limits
Access Planning	285	Req	Access Planning	Plan Protection Limits
Access Planning	286	Req	Access Planning	Plan Protection Limits
Access Planning	288	Req	Access Planning	Plan Protection Limits
Access Planning		**Heading**	**Access Planning**	**Plan Possession**
Access Planning	045	Req	Access Planning	Plan Possession
Access Planning	084	Req	Access Planning	Plan Possession
Access Planning	162	Req	Access Planning	Plan Possession
Access Planning	163	Req	Access Planning	Plan Possession

Access Planning	165	Req	Access Planning	Plan Possession
Access Planning	166	Req	Access Planning	Plan Possession
Access Planning	171	Req	Access Planning	Plan Possession
Access Planning	172	Req	Access Planning	Plan Possession
Access Planning	173	Req	Access Planning	Plan Possession
Access Planning	174	Req	Access Planning	Plan Possession
Access Planning	175	Req	Access Planning	Plan Possession
Access Planning	176	Req	Access Planning	Plan Possession
Access Planning	177	Req	Access Planning	Plan Possession
Access Planning	210	Req	Access Planning	Plan Possession
Access Planning	211	Req	Access Planning	Plan Possession
Access Planning	306	Req	Access Planning	Plan Possession
Access Planning	343	Req	Access Planning	Plan Possession
Access Planning	348	Req	Access Planning	Plan Possession
Access Planning	354	Req	Access Planning	Plan Possession
Access Planning	355	Req	Access Planning	Plan Possession
Access Planning	356	Req	Access Planning	Plan Possession
Access Planning	357	Req	Access Planning	Plan Possession
Access Planning	358	Req	Access Planning	Plan Possession

Access Planning	359	Req	Access Planning	Plan Possession
Access Planning		**Heading**	**Access Planning**	**Planning Automation**
Access Planning	272	Req	Access Planning	Planning Automation
Access Planning	273	Req	Access Planning	Planning Automation
Access Planning	274	Req	Access Planning	Planning Automation
Access Planning	275	Req	Access Planning	Planning Automation
Access Planning	276	Req	Access Planning	Planning Automation
Access Planning	277	Req	Access Planning	Planning Automation
Access Planning	278	Req	Access Planning	Planning Automation
Access Planning		**Heading**	**Access Planning**	**Visualisations**
Access Planning	135	Req	Reporting	Visualisations
Access Planning	289	Req	Reporting	Visualisations
Access Planning	290	Req	Reporting	Visualisations
Access Planning	291	Req	Reporting	Visualisations
Access Planning	292	Req	Reporting	Visualisations
Access Planning	293	Req	Reporting	Visualisations
Access Planning	294	Req	Reporting	Visualisations
Access Planning	295	Req	Reporting	Visualisations
Access Planning	296	Req	Reporting	Visualisations
Access Planning	297	Req	Reporting	Visualisations
Access Planning	299	Req	Reporting	Visualisations
Access Planning	300	Req	Reporting	Visualisations
Access Planning	301	Req	Reporting	Visualisations

Access Planning	302	Req	Reporting	Visualisations
Access Planning	303	Req	Reporting	Visualisations
Access Planning	304	Req	Reporting	Visualisations
Access Planning	305	Req	Reporting	Visualisations
Access Planning		**Heading**	**Access Planning**	**Plan/Book Train Formations**
Access Planning	059	Req	Access Planning	Plan/Book Train Formations
Access Planning	060	Req	Access Planning	Plan/Book Train Formations
Access Planning	220	Req	Access Planning	Plan/Book Train Formations
Access Planning	221	Req	Access Planning	Plan/Book Train Formations
Access Planning	222	Req	Access Planning	Plan/Book Train Formations
Access Planning	223	Req	Access Planning	Plan/Book Train Formations
Access Planning	224	Req	Access Planning	Plan/Book Train Formations

Access Planning	225	Req	Access Planning	Plan/Book Train Formations
Train Pathing		**Heading**	**Access Planning**	**Path Trains (Not in Passenger Service)**
Train Pathing	063	Req	Access Planning	Path Trains (Not in passenger service)
Train Pathing	064	Req	Access Planning	Path Trains (Not in passenger service)
Train Pathing	065	Req	Access Planning	Path Trains (Not in passenger service)
Train Pathing	066	Req	Access Planning	Path Trains (Not in passenger service)
Train Pathing	067	Req	Access Planning	Path Trains (Not in passenger service)
Train Pathing	068	Req	Access Planning	Path Trains (Not in Passenger Service)
Train Pathing	069	Req	Access Planning	Path Trains (Not in Passenger Service)
Train Pathing	070	Req	Access Planning	Path Trains (Not in Passenger Service)
Train Pathing	071	Req	Access Planning	Path Trains (Not in Passenger Service)
Train Pathing	072	Req	Access Planning	Path Trains (Not in Passenger Service)
Train Pathing	073	Req	Access Planning	Path Trains (Not in Passenger Service)
Train Pathing	077	Req	Access Planning	Path Trains (Not in Passenger Service)
Train Pathing	091	Req	Access Planning	Path Trains (Not in Passenger Service)
Train Pathing	092	Req	Access Planning	Path Trains (Not in Passenger Service)
Train Pathing	093	Req	Access Planning	Path Trains (Not in Passenger Service)
Train Pathing	161	Req	Access Planning	Path Trains (Not in Passenger Service)

Train Pathing	341	Req	Access Planning	Path Trains (Not in Passenger Service)
Train Pathing	362	Req	Access Planning	Path Trains (Not in Passenger Service)
Access Planning		**Heading**	**Access Planning**	**Manage Opportunity Works**
Access Planning	189	Req	Access Planning	Manage Opportunity Works
Access Planning	190	Req	Access Planning	Manage Opportunity Works
Access Planning	191	Req	Access Planning	Manage Opportunity Works
Access Planning	192	Req	Access Planning	Manage Opportunity Works
Access Planning	340	Req	Access Planning	Manage Opportunity Works
Access Planning		**Heading**	**Approval**	**Book Critical Protection Staff Resources**
Access Planning	226	Req	Access Planning	Book Critical Protection Staff Resources
Access Planning	227	Req	Access Planning	Book Critical Protection Staff Resources
Access Planning	228	Req	Access Planning	Book Critical Protection Staff Resources
Access Planning	229	Req	Access Planning	Book Critical Protection Staff Resources
Access Planning	230	Req	Access Planning	Book Critical Protection Staff Resources
Access Planning	231	Req	Access Planning	Book Critical Protection Staff Resources

Access Planning	232	Req	Access Planning	Book Critical Protection Staff Resources
Access Planning	233	Req	Access Planning	Book Critical Protection Staff Resources
Access Planning	234	Req	Access Planning	Book Critical Protection Staff Resources
Access Planning	235	Req	Access Planning	Book Critical Protection Staff Resources
Access Planning	236	Req	Access Planning	Book Critical Protection Staff Resources
Access Planning	237	Req	Access Planning	Book Critical Protection Staff Resources
Access Planning	238	Req	Access Planning	Book Critical Protection Staff Resources
Access Planning		**Heading**	**Access Planning**	**Book Specialist Equipment Availability**
Access Planning	239	Req	Access Planning	Book Specialist Equipment Availability
Access Planning	240	Req	Access Planning	Book Specialist Equipment Availability
Access Planning	241	Req	Access Planning	Book Specialist Equipment Availability
Access Planning	242	Req	Access Planning	Book Specialist Equipment Availability
Access Planning		**Heading**	**Access Planning**	**Manage Notifications of Clashes**
Access Planning	043	Req	Access Planning	Manage Notifications of Clashes

Access Planning	044	Req	Access Planning	Manage Notifications of Clashes
Access Planning	094	Req	Access Planning	Manage Notifications of Clashes
Access Planning	095	Req	Access Planning	Manage Notifications of Clashes
Access Planning	096	Req	Access Planning	Manage Notifications of Clashes
Access Planning	097	Req	Access Planning	Manage Notifications of Clashes
Access Planning	098	Req	Access Planning	Manage Notifications of Clashes
Access Planning	099	Req	Access Planning	Manage Notifications of Clashes
Access Planning	101	Req	Access Planning	Manage Notifications of Clashes
Access Planning	102	Req	Access Planning	Manage Notifications of Clashes
Access Planning	103	Req	Access Planning	Manage Notifications of Clashes
Access Planning	104	Req	Access Planning	Manage Notifications of Clashes
Access Planning	112	Req	Access Planning	Manage Notifications of Clashes
Access Planning	182	Req	Access Planning	Manage Notifications of Clashes
Access Planning	318	Req	Access Planning	Manage Notifications of Clashes

Access Planning		**Heading**	**Access Planning**	**Resolve Clashes and approval of clashes or joint working**
Access Planning	074	Req	Access Planning	Resolve Clashes and approval of clashes or joint working
Access Planning	088	Req	Access Planning	Resolve clashes and approval of clashes or joint working
Access Planning	105	Req	Access Planning	Resolve Clashes and Approval of Clashes or Joint Working
Access Planning	106	Req	Access Planning	Resolve Clashes and Approval of Clashes or Joint Working
Access Planning	107	Req	Access Planning	Resolve Clashes and Approval of Clashes or Joint Working
Access Planning	108	Req	Access Planning	Resolve Clashes and Approval of Clashes or Joint Working
Access Planning	109	Req	Access Planning	Resolve Clashes and Approval of Clashes or Joint Working
Access Planning	110	Req	Access Planning	Resolve Clashes and Approval of Clashes or Joint Working
Access Planning	111	Req	Access Planning	Resolve Clashes and Approval of Clashes or Joint Working
Access Planning	181	Req	Access Planning	Resolve Clashes and Approval of Clashes or Joint Working
Access Planning		**Heading**	**On Night**	**Plan TC Switching Time Changes**
Access Planning	243	Req	Access Planning	Plan TC Switching Time Changes
Access Planning	244	Req	Access Planning	Plan TC Switching Time Changes

Access Planning	245	Req	Access Planning	Plan TC Switching Time Changes
Access Planning	246	Req	Access Planning	Plan TC Switching Time Changes
Access Planning	247	Req	Access Planning	Plan TC Switching Time Changes
Access Planning	248	Req	Access Planning	Plan TC Switching Time Changes
Access Planning	249	Req	Access Planning	Plan TC Switching Time Changes
Access Planning	250	Req	Access Planning	Plan TC Switching Time Changes
Access Planning	251	Req	Access Planning	Plan TC Switching Time Changes
Access Planning	345	Req	Access Planning	Plan TC Switching Time Changes
Access Planning	346	Req	Access Planning	Plan TC Switching Time Changes
Access Planning		**Heading**	**Access Planning**	**Plan TC switching time changes (Cancel EH)**
Access Planning	310	Req	Access Planning	Plan TC switching time changes (Cancel EH)
Access Planning		**Heading**	**Approval**	**Planning Approval (Lockdown)**
Access Planning	311	Req	Approval	Planning Approval (Lockdown)
Access Planning	313	Req	Approval	Planning Approval (Lockdown)
Access Planning	314	Req	Approval	Planning Approval (Lockdown)
Access Planning		**Heading**	**Approval**	**Planning Assurance**
Access Planning	204	Req	Approval	Planning Assurance
Access Planning	205	Req	Approval	Planning Assurance
Access Planning	206	Req	Approval	Planning Assurance
Access Planning	207	Req	Approval	Planning Assurance
Access Planning	208	Req	Approval	Planning Assurance
Access Planning	209	Req	Approval	Planning Assurance

Access Planning	215	Req	Approval	Planning Assurance
Access Planning	216	Req	Approval	Planning Assurance
Access Planning	217	Req	Approval	Planning Assurance
Access Planning	218	Req	Approval	Planning Assurance
Access Planning	219	Req	Approval	Planning Assurance
Publications		**Heading**	**Publish**	**Publish**

Publications	193	Req	Publish	Publish
Publications	194	Req	Publish	Publish
Publications	195	Req	Publish	Publish
Publications	196	Req	Publish	Publish
Publications	197	Req	Publish	Publish
Publications	198	Req	Publish	Publish
Publications		**Heading**	**Reporting**	**Reporting**
Publications	046	Req	Reporting	Reporting
Publications	307	Req	Reporting	Reporting
Publications	349	Req	Reporting	Reporting
Publications	360	Req	Reporting	Reporting
Access Planning		**Heading**	**On Night**	**Confirm Access Opportunity**
Access Planning	308	Req	On Night	Confirm Access Opportunity

Access Planning	309	Req	On Night	Confirm Access Opportunity
System Admin	123	Req	System Admin	System Admin
System Admin	124	Req	System Admin	System Admin
System Admin	125	Req	System Admin	System Admin
System Admin	126	Req	System Admin	System Admin
System Admin	127	Req	System Admin	System Admin
System Admin	128	Req	System Admin	System Admin
System Admin	129	Req	System Admin	System Admin
System Admin	130	Req	System Admin	System Admin
System Admin	131	Req	System Admin	System Admin
System Admin	132	Req	System Admin	System Admin
Access Planning		**Heading**	**Access Planning**	**Data Structure**
Access Planning	038	Req	Access Planning	Data Structure
Access Planning	039	Req	Access Planning	Data Structure
Access Planning	040	Req	Access Planning	Data Structure
Access Planning	041	Req	Access Planning	Data Structure
Access Planning	042	Req	Access Planning	Data Structure
Access Planning	120	Req	Data Structure	Data Structure

Access Planning	121	Req	Data Structure	Data Structure
Access Planning	122	Req	Data Structure	Data Structure
Access Planning	178	Req	Data Structure	Data Structure
Access Planning	252	Req	Data Structure	Data Structure
Access Planning	253	Req	Data Structure	Data Structure

Access Planning	254	Req	Data Structure	Data Structure
Access Planning	255	Req	Data Structure	Data Structure
Access Planning	256	Req	Data Structure	Data Structure
Access Planning	257	Req	Data Structure	Data Structure
Interface	150	Req	Interfaces	Interface to Access Control System
Interface	151	Req	Interfaces	Interface to Access Control System
Interface	152	Req	Interfaces	Interface to Access Control System
Interface	153	Req	Interfaces	Interface to Access Control System
Interface	154	Req	Interfaces	Interface to Access Control System
Interface	155	Req	Interfaces	Interface to Access Control System
Interface	156	Req	Interfaces	Interface to Access Control System
Interface	157	Req	Interfaces	Interface to RTS (Timetabling System)
Interface	158	Req	Interfaces	Interface to RTS (Timetabling System)
Interface	159	Req	Interfaces	Interface to RTS (Timetabling System)
Interface	160	Req	Interfaces	Interface to Route Availability Information

Interface	183	Req	Interfaces	Interface to CTAC (Access Control System)
Interface	184	Req	Interfaces	Interface to Permit Access System (Access Control System)
Interface	186	Req	Interfaces	Interface to OGMS (Access Resource Management System)
Interface	187	Req	Interfaces	Interface to Geographic Systems
Interface	188	Req	Interfaces	Interface to Station Diagrams
Interface	363	Req	Interfaces	Interface to 3rd Party Systems

lanning Functional Requirements

Description
The objective is to allow access requestor to define their own programmes and manage the role who can create projects within a programme. This reduces the effort required from the Access Dept. to support this element of the process. Capturing this data correctly will help deliver a more accurate and supportable system and introduce better management of self serve where possible. **A typical Programme team would comprise of:** **- a sponsor** **- a programme manager** **- 1 or more project managers who would create access plans and submit access requests** **- 1 or more access requesters who would submit access requests using supplied**

The solution shall enable sponsor roles to be created.

The solution shall enable each sponsor to create the following entities: Programme, Project

The solution shall enable each sponsor to add roles to each project or programme.

The solution shall enable each role responsible for a project or programme to delegate responsibility to other roles if required.
The system shall be able to assign delegated role responsibilities as described in requirements 001, 002, 003 and 004 for programme, projects, access plan creators and
The solution shall batch import project and programme roles and corresponding metadata.

The solution shall use the TfL Active Directory to look up internal TfL employees.

Where users of the solution are non TfL employees the system shall be able to create user accounts for these users outside of AD.
The solution shall capture the following information at the programme level, this list is not exhaustive:
- Programme Unique ID
- UIP Code (for cost charging)
- SAP Cost centre
- The portfolio that the Programme is part of
- Personal Information on the person responsible for the programme
- Personal Information on the designated contact for the programme (email, telephone no, Name ...)
- Description of the programme
- Related Programme documents
- Budget Milestones

The solution shall be delivered as a web based client application for all data capture functions performed by the access requestors.

The objective is to allow access requestor to define their own projects and manage the role who can create Access Plans within a project. This reduces the effort required from the Access Dept. to support this element of the process. Capturing this data correctly will help deliver a more accurate and supportable system and

The solution shall capture the following information at the project level, this list is not exhaustive:

- Project Unique ID
- The Programme that the project is part of
- UIP Code (for cost charging)
- SAP Cost Centre
- Personal Information on the person responsible for the programme
- Personal Information on the designated contact for the programme (email, telephone no, Name ...)
- Description of the project
- Related project documents
- Budget Milestones

The objective is to enable all work planned on the railway or in stations to be visible to the access department and access planning system. The concept of an access plan aligns with the internal TfL governance process (Pathway) and ensures that all work whether it be maintenance, simple or complex project work is captured and

The solution shall capture the following information in the access plan:

- The Programme/Project that the access plan refers to
- The Work Description
- Information about specialist resource requirements
- Track location(s) at which the work is planned to take place at
- Specific station locations and rooms in which the work is proposed to take place
- Specific information on the stations at which the track will require access from
- Shift related information describing the availability of the access requests team to carry out the described work
- Specific protection resources required
- Specific plant, equipment and trains required to carry out the work

The solution shall make use of visual tools such as a calendar to enable the requestor to select a given time span to carry out work between.

The solution shall make use of visual tools such as track line diagrams to enable the access requester to select a more precise location of the track that the work is planned to take

The solution shall show the planned closures and other work present if a requester chooses a date and location where there is a potential overlap.

The solution shall present the next available geographic and time slot for the work to take place to the requester, offering EH where possible and check the appropriate resources are

The objective is to allow the access planning function within the access department to review the plans for work on the infrastructure. The purpose being to direct the work to the relevant and most efficient method of planning. I.e. some work requires very little planning and so can be self-served, other require heavy interactions with

The solution shall warn the access team of any outstanding decisions and or approvals required for submitted access plans that have not been dealt with within the agreed SLAs

The solution shall provide case management style functionality to be able to track an access plan through its life (conception as an access request as part of a project and programme through to a access request and then a planned piece of access that is agreed

The solution shall clearly show where in the time line the request for work is. I.e. what stage of request, planning, assurance or publications the work is at.
The solution shall allow the access planner who is reviewing the request to assign free text comments to each proposed access plan.
The system shall allow the planners to create specific request booking forms that are suitable for the work they describe.
The solution shall enable the access team planners to use an existing access request template to assign to the access requesters access plan.
The solution shall store access request templates for the access planner to assign to the access plan. This helps to direct the requester to submit the most fit for purpose access
The solution shall store template access plans to help direct the requester to the most fit for purpose plan for the work they intend to carry out.
The solution shall allow all users to share global templates for access plans and access requests.
The solution shall allow requesters to save partially populated templates and reuse them at any time within the access plans validity period.
The system shall be able to capture the following information within a template. See Appendix L Ref-057. Some of the main section of information are listed below:
- define time start and end
- shift patterns
- define location
- define work description
- define work type
- system defines access type
- define hazards (ie.hot works)
- phases of activities
- protection resources required
- Site access
- materials (delivery, storage, waste)
- Trains or other vehicles
- Storage and hording licences

(final field list to be decided in design phase)
The system shall contain the functionality for templates to hide information not applicable to the booking type. I.e. station booking to not contain any track or train booking information.
The system shall deliver templates to pre populate certain fields and pick lists from information contained within the Access Plan that can be further modified by the user . I.e.
The system shall contain lock sections of information brought in from the related access plan that can be viewed within the access request but not modified. This information is shown for information purposes and completeness of the access request.
The system shall contain the functionality for template to be allocated to a workflow. Workflow and times scales will be dependant on specific criteria entered in the access
The system shall be able to apply field validation to forms and templates.

Railway or station closures may be required to complete project or maintenance work. Closures involve impacting the paying customer and so a level of approval from local government and customers may be required. This is managed by a department outside of the Access Department. This department may have to carry out modelling simulations to look at alternatives and impacts. The access planning

The system shall integrate with the internally developed Events & Closures System. The current system is an MS Access 2010 database front end connected to a SQL server back end. We can provide more technical information if required. We are interested in understanding the feasibility of integrating these requirements into the planning solution.
Closure information shall contain the following for all approved closures:
- Access Closure ID (If applicable)
- S&SD Closure ID
- Closure Name
- Infrastructure Closed (LU, NR, Overground, DLR, TfL Streets etc.)
- Closure TfL S&SD SPOC
- Closure Project Manager (Primary Work)
- Primary Work Overview/Description
- Closure Start Date/Time (Timespan)
- Closure End Data/Time (Timespan)
- Primary affected locations (LCS Codes, Start Date/Time, End Date/Time to allow a closure to shrink and grow over the timespan)
- Protected Routes (LCS Codes)
- Station/Track Locations (Primary location of closure)
- Status of Closure

See Appendix L Ref-039 for an example of the current closure information extracted from the Closures Database.

External events within London are captured by another system and so access planner and requesters must be made aware of such events as them will affect how the railway should operate at or around the event locations on the specific day.

The system shall integrate with the internally developed Events & Closures System. The current system is an MS Access 2010 database front end connected to a SQL server back end. We can provide more technical information if required. We are interested in understanding the feasibility of integrating these requirements into the planning solution.
Event information shall contain the following:
- Event ID
- Event Type (Football, Music, Festival, Dummy for modelling etc.)
- Event Name
- Event Venue
- Expected Attendance
- Event TfL SPOC
- Event Start Date/Time (Hard/Soft Times)
- Event End Data/Time (Hard/Soft Times)
- Event affected locations (LCS Codes)
- Protected Routes (LCS Codes)
- Station/Track Locations (Primary location to access the event)
- Status of Event

Soft Times relate to events where attendees arrive and depart over a prolonged period e.g. an all day music event. Hard times relate to events where attendees mostly arrive and leave together. e.g. a football match.
See Appendix L Ref-039 for an example of the current event information extracted from the

The system shall supply notification of:
- New events
- Cancelled or postponed events
- Change of key event information including start date/time, protected routes etc.)
(final field list to be decided in design phase)
The Access Planning System shall geographically display events information.
The Access Planning System shall geographically display closure information for both approved and unapproved closures.
The system shall notify the planner who has planned a piece of work if an event changes and affects existing booked work.
The objective is to allow both access planners and access requesters the ability to view other work that may be occurring (draft or approved) on the infrastructure to
The Access Planning System shall geographically display works information for both approved and pipeline work requests and bookings.
The system shall have visibility of all planned and pipeline work and filter or highlight by the different categories below:
- Planned Maintenance
- Possessions
- Specified Areas
- Engineers Current Areas
- Worksites that prevent others from working in the same area
- Worksites that restrict work that other can do in the same area
- Worksites that place no restrictions on others
- Engineering train moves
- Stock moves
- Out stabled trains
- Other closures
All track work must be defined using a track booking. The booking will contain all the relevant information for the access planning system and department to ensure the
The system shall be able to capture the following information on a track booking:
- Start TCS
- End TCS
- Start Date/Time
- End Date/Time
- Booking description
- Booking Short Description (Name)
- Whether the work restricts others from the type of work they will undertake or prevents others from doing any work within the area
- Booking Status

Appendix L Ref-017 is an example of the existing access booking form used. Appendix M is an example of the structure and content of an access booking form.
(final field list to be decided in design phase)
The system shall be able to create repeated booking by allowing the requester to create the following:
- Recurrence Pattern
    - Daily, Weekly, Monthly, Annually
    - Recur every N Weeks on (Mon, Tues, Wed, Thurs, Fri, Sat and Sun)
    - Start Date
    - End Date, End after N occurrences, No End Date.

The system shall be able to allocate a priority to a booking type to ensure the bookings are managed accordingly and not cancelled without consultation. e.g. track and stations maintenance may have a higher priority than other bookings. I.e. they cannot just be **programme. The submitted and draft requests should be visible to all members of the programme team.**
The system shall allow the requester to submit a new work request.

The access input screen shall only allow work requests to be raised against predefined projects/programmes and existing access plans. If project does not exist the requestor will need to request that the project is added via the administrator.
The system shall be able to save 'draft' access requests before submitting.

The work requester shall be able to delete a draft access request.

The system shall allow the user to create a new access request from a copy of a previously submitted request.
The system shall allow the user to view requests that they have already submitted and are in draft status.
The system shall allow the user to submit access requests.

The system will validate any mandatory fields upon submission of access requests.

The system shall generate a unique access request number when the request is submitted, provided that the access request does not already have a unique reference number from
The system shall determine if the request is outside the limits of the predefined submissions dates. The submission dates will very depending on the nature of the work. If these dates are broken the submission is recorded as urgent and will follow a different workflow.
The system shall generate lockdown email reminder based on the start date of the work request window and other fields still to be defined.
The system shall lock the access request so that the requester can no longer edit the record once submitted.
The system shall generate an email back to the requestor to confirm that the access request has been submitted.
The system shall allow the requester to be able to search for previously submitted access requests and retrieve a read only copy of the request.
The system shall allow a access request to contain one or more worksites, The worksites do not need to be contiguous.
The system shall allow the user to create a track access request from a allocated template.

The system shall allow the user to select the location they wish to access by reference to one or more of:
- a proportional track layout map
- traction current section diagram
The system shall allow the user to book areas:
- by lassoing or selecting on a map/diagram (to accurately define the worksite in geographic terms)
The system shall present to the user a cascading list of bookable sections i.e., Line, Station, Platform and TCS.

The system shall allow access planners to unlock a submitted request for further editing and re-submission.
The system shall allow the planner to change one of the dates within the repeated booking described in Req057 without changing the overall pattern of bookings.
All station work must be defined using a station booking. The booking will contain all the relevant information for the access planning system and department to ensure the work can be successfully delivered.
The system shall allow the user to create a station access request from a allocated template.
The system shall allow the user to select the location they wish to access by reference to a station map, via a series of cascading dropdown lists or both.

The system shall present to the user a cascading list of bookable areas i.e., zones, rooms, platforms.
The type of planning and approvals required for different access and work to be carried out on the railway will require different levels of planning and approvals. These should be defined within a number of business rules.
The solution shall send reminder emails to individuals who have not completed a given task in the allotted time as a reminder.
The system shall be able to administer the following workflows:
- No approval workflow, not considered in planning meetings (requester notified of overlapping work)
- No approval workflow, considered in the planning meetings
- Approval workflow, internal review only by the access planning team
- Approval workflow, internally planned by the access planning teams

The system shall be able to assign a workflow to a access request template.

The system shall be able to assign an access request template to an access plan or activities within an access plan.
The administrator shall be able to create or modify existing workflows. See Appendix H for examples of the workflows required to be created for the Access Planning System.
The administrator shall be able to modify existing workflow parameters. i.e. roles, timescales.
A closure is where an asset is affected such that there is an impact to the general public i.e. an escalator taken out of service for maintenance or and activity may take longer than the engineering hours and therefore impact the next day timetable. Defining the scope and limits of a closure and understanding the geographic and
The system shall allow the creation of closures.

A closure shall contain the following information:
- Access Closure ID
- Closure Name
- Infrastructure Closed (LU, NR, Overground, DLR, TfL Streets etc.)
- Closure TfL S&SD SPOC
- Closure Project Manager (Primary Work)
- Primary Work Overview/Description
- Closure Start Date/Time (Timespan)
- Closure End Data/Time (Timespan)
- Primary affected locations (LCS Codes, Start Date/Time, End Date/Time to allow a closure to shrink and grow over the timespan)
- Protected Routes (LCS Codes)
- Station/Track Locations (Primary worksite of the closure)
- Status of Closure
- Closure Type (e.g. Major, Minor, L&E)
- Related Possession IDs
- Primary Work Request ID
- Work Request IDs of other work within closure

(final field list to be decided in design phase)
The system shall allow closures limits to be entered geographically.

A closure is where an asset is affected such that there is an impact to the general public i.e. an escalator taken out of service for maintenance or and activity may take longer than the engineering hours and therefore impact the next day timetable. Where a closure exists approval of the closure is required from other parties such as
The system shall pass the following information to the S&SD Closures System:
- Access Closure ID
- Closure Name
- Infrastructure Closed (LU, NR, Overground, DLR, TfL Streets etc.)
- Closure TfL S&SD SPOC
- Closure Project Manager (Primary Work)
- Primary Work Overview/Description
- Closure Start Date/Time (Timespan)
- Closure End Data/Time (Timespan)
- Primary affected locations (LCS Codes, Start Date/Time, End Date/Time to allow a closure to shrink and grow over the timespan)
- Station/Track Locations (Primary worksite of the closure)

(final field list to be decided in design phase)

The system shall receive the following information from the S&SD Closures System for all approved closures:
- S&SD Closure ID
- Access Closure ID
- Infrastructure Closed (LU, NR, Overground, DLR, TfL Streets etc.)
- Closure TfL S&SD SPOC
- Primary Work Overview/Description
- Closure Start Date/Time (Timespan)
- Closure End Data/Time (Timespan)
- Primary affected locations (LCS Codes, Start Date/Time, End Date/Time to allow a closure to shrink and grow over the timespan)
- Protected Routes (LCS Codes)

The system shall provide case management capability as described in Appendix A.

Some of the required access does not always require internal planning by the access department. If enough detail describing the extent of the booking is captured and understood these bookings can be automatically approved by the system.

The system shall be able to deliver the auto approve booking business rules as described in Appendix H, IDs 3 and 4.

Maintenance on the underground within stations and track areas shall be booked way in advance and repeated on a timeframe defined by the engineering maintenance standards for the asset.

The solution shall enable the requester to modify the frequency of the reoccurring maintenance activities for a chosen date forward in time without affecting the dates prior to this time.

The solution shall deliver a set of template maintenance activities with the functionality to request and book cyclical maintenance (maintenance that repeats at a given interval for a given time period, usually indefinitely until changed).

The system shall allow maintenance schedules to be uploaded as CSV files. (final field list to be decided in design phase)

The system shall allow the requesters to enter a maintenance task directly into the system.

As part of the planning process, the limits in which to work to be undertaken are required to be defined and understood by the planning system. The worksite limits are the geographic limits of the actual work and not the protection required to safely

The system shall allow the track planners or possessions planners to define worksites limits directly onto a track diagram.

The system shall allow the planner to select the worksite limits on a map.

The system shall ensure that the worksite limits are greater than or equal to the limits of the

The system shall allow the planner to select a worksite with 1m resolution.

The solution shall enable requests for access to be 'put on a shelf' if they are not able to be planned at this present moment in time. These requests can be called upon at any point

The system shall allow stations planners to directly make station bookings onto the station

The system shall be able to capture the likelihood or intent for a piece to overrun into traffic-hours. This could be used as useful information for the Access Control System on the

The system shall ensure that planners can be kept informed of changes that may affect

The solution shall be able to suggest permutations of plans where the effect on the railway

The solution shall flag up where there are potential resource saving opportunities. Such as sharing the same train to get equipment to site or sharing the same protection resources.
Work shall be able to be manually planned where appropriate and aided by a planning tool if rules can be understood and reproduced.
The planner should be able to make changes to existing plans and look at the effect of a change to other work plans occurring at similar times and locations.
The system shall be able to assign an approximate cost of the booking for the purposes of cost benefit analysis if work is required to be changed or cancelled.
The system will calculate the cost of the booking using the following:
- Cost of the work taken from the project/programme or maintenance schedule
- Cost or weighting of the access human resources required to deliver the booking
- Cost of the trains required to support the booking.

The system can weight the cost of the access human resource using the following criteria but not limited to:
- Self served booking
- Booking at station
- Booking on track
- Access planned booking on track
- Access planned booking on station
- Booking in a Possession
- Booking in a Closure
- Booking Requiring a Train
- Required to meet maintenance standard

When a piece of work is moved or cancelled the system shall be able to calculate the total cost of the work not taking place and inform the planner. This information shall be used to help plan work when critical decisions are required to be made regarding moving or
The system shall log the owner and project/programme that the cancelled work belongs to such that a record can be kept of which parties are impacted the most from cancellations and change. This will help the planner spread the pain when it comes to cancelling work
The system shall define a track booking as:
-Line(s)
-Worksite from location (geographic)
-Worksite to location (geographic)
-Affected TCSs
-Additional TCSs required for protection
-Start Date
-End Date
-Engineering Hours (EH)
-Traffic Hours (TH)
-Both EH and TH
(final field list to be decided in design phase)

Worksite limits are defined by fixed geographic points e.g.:
- Stations
- Platforms
- Signals
- Traction current gaps
- Line
- Bridges
- Roads
- Points/P&Cs

(final field list to be decided in design phase)
The system shall be able to action an email based on the output of a business rule.
The system shall show the make the following information available to the roles who use the access planning system. See appendix I for a list of the information required for access
The system shall allow the planners to record notes applicable to locations on the geographic infrastructure that can be shared.
In any situation where a new possession plan from either a template or another plan you need to be warned of any version changes in the geography.
The system shall highlight all bookings of all statuses affected by a change in the underlying
The system shall be able to hold a catalogue of other non protection resources such as Technical Officers (TOs)and Cable Linesmen (CBL).This information is currently help outside of the department.
The system must allow for 'exclusive/OR' relationships between assets and/or locations. For example, only escalator 1, 2 OR 3 can be closed at the same time. If an escalator is closed at Green Park then you cannot close one at Victoria. This table should be configurable by
The system shall warn the access planner of any critical assets that cannot be worked on (closed for operation use) when they are operationally sensitive to an existing closed asset.
The work being carried out on the railway may require additional geographic limits to ensure that the work can be safely protected. The limits of such protection are
The system shall allow the track planners or possessions planners to define protection limits directly onto a track diagram.
The system shall suggest limits of protection if no additional protection limits to work required based on nearest TC gap, headway boards, point ends, signal (MST type signal), sign posts for moving block signalling. This functionality will act like a snap to protection
The system shall select the TC sections that cover the worksite for line clear and line safe protection in engineering hours as the protection limits. The system will snap to TC
The system shall allow the planner to select the worksite protection limits on a map.
The system shall allow the planner to select a worksite protection limits with 1m resolution.
The system shall ensure that the worksite protection limits are adjacent to the worksite.
The system shall allow the access planner to specify protection limits manually to a location
One of the may methods of protecting and managing access onto the track is to carry out work within a possession. The detailed information required to plan and
All possession planning shall be planned within the accuracy of 1 minute resolution.
The system shall be able to add additional protection to adjacent parts of the line near worksites. E.g. passenger trains will be running through the night due to night tube.
The different stages of a possession shall be able to be captured in the planning process.
The possession stages must be distinguishable on the track diagram visualisations. I.e. different colours representing the different stages and the stages only be applicable on the

The system shall allow the system admin role to modify the geography if a major asset has been removed and the geography is still showing the asset present. I.e. mark a set of points as removed. The system will stop the planners booking work over this asset.
The system shall allow worksite milestones to be defined within a given worksite. Each milestone can have a name and target date/time.
The system shall allow a possession planner to select one or more worksites as the primary worksites for the possession.
The system shall make the possession description the same description as the primary worksite description. The possession planner can change the possession description once
The system must not allow the worksite and its protection limits to be greater than the possession limits. The possession limits shall not be greater than the closure limits. If this occurs the system shall warn the planner and upon acknowledgement allow the possession
The system shall allow multiple stages of a possession to be created. E.g. a possession may start off on the first day as big to ensure a train can enter, then reduce in size for a number of days to the limits of the work, finally the possession may increase on the last day
The system shall associate a timetable version with a possession. Note certain parts of the railway may have more than one timetable as they share the same track in places. I.e.
The system shall inform the possession planner if the underlying timetable that exists is changed when in planning stage.
The system shall clash check worksites within a possession and inform the possession planner of any potential conflicts.
The system shall allow planners to promote a possession plan as a reusable template.
The system shall allow a new possession plan to be created from:
- the possession plan template library
- existing possession plans that are within similar geographic limits from the library.
- an empty plan.
The system shall be able to include detailed possession planning diagrams of the specific track locations within a possessions plan report.
The system shall allow planners to add access related assets to the geography. E.g. traction current gap bridging plates which can be re used as locations to split the traction
The system shall be able to reuse existing possession plans for similar or exactly the same geographic areas. The user shall be able to specify which elements of the plan are reused i.e. the whole possession including worksites and work or only the possession limits
The system shall allow protection staff to indicate they have arrived at the worksite.
The system shall allow the possession planner to indicate the location that protection equipment should be placed for the possession. Protection equipment would include:
- Possession Limit Marker Boards (PLMBs)
- Traction Current Marker Boards (TCMBs)
- Worksite Limit Marker Boards (WLMBs)
- Lamps
- Detonators
- Scotches and clips for securing points (different scotches and clips maybe required for specific points)
- A secured train.
The system shall allow the possession planner to temporary rename a signal for the
The system shall limit the type of scotch and clip required for a possession based on the type of points on the network. See Appendix L Ref-060
The system shall allow the possessions planner to annotate the possessions planning

The system shall allow the possessions planner to measure a distance from the top of the platform ramp and show this on the diagram. This is used for to define the location of specific equipment required in the possession planning process.

With the access planning process being fully captured within a planning system it may be possible to automate some of the existing manual planning tasks to speed up and improve the existing planning process.

The system shall be able to automatically plan worksites and worksite protection tasks into
The system shall be able to suggest alternative schedules of selected bookings and allow the planner to choose which option to use.
The system shall be able to allocate opportunity works within a set of planned worksites or possessions by looking for work than exists within a user selected timeframe.
The system shall present to the planner appropriate opportunity work that could be planned together. Opportunity works is work that can exist along side other work and occur at the same time as other work. This may involve moving some work by 1 week to accommodate
The system shall suggest to the planner where protection limits can be shared between
The system will allow the planner to lock planned work and therefore remove the locked work from any automatic scheduling.
The system shall clash check bookings and highlight work that cant occur alongside one another whilst the planner is planning the work.

To visually plan and report on information within the access planning system is critical to designing a successful and efficient access plan.

The system shall be able to present access information in a visualisation based report for use by the access planners and access requesters. See Appendix F and Appendix J for examples of the different visualisation techniques that could be used for the different roles
The system shall be able to visualise station booking in a stations calendar type view. See
The system shall allow the user to interrogate a station or track book and look at the complete booking details. See Appendix F1.2. and F2.1 for a screen shot of the detailed
The system shall be able to distinguish the different access booking types or categorise of access in the track and station visualisations. See appendix F.
The system shall be able to filter the track and station visualisations by access types, access categories and other appropriate data types.
The system shall allow the user to view future dates and past dates of access bookings or planned access. See appendix F for some of the screen shots of a prototype describing how the access can be viewed for different days, weeks and months.
The system shall be able to show all status access requests and bookings and allow the user to filter between or show all.
The system shall be able to show access bookings within a station that have a specific
The system shall be able to show track access bookings against the traction current
The system shall be able to show all track bookings against the location they are planned to occur at. This can be visualised as a time location grid. See Appendix F for a track grid
The system shall show more than one booking on a given day at the same location on the visualisation and allow the user to understand there is more than one booking present. See Appendix F for examples of how multiple booking can be visualised using "counts" of
The system shall be able to visualise events within London geographically showing the status of the event i.e. planned or actual along with the designated protected route for the venue. A venue may have one or more protected routes dependant on the size of the
The system shall be able to visualise track bookings and events in a track diagram type view. This view will show the actual track sections that the work is booked on. Other layer can be seen in such a view such as signals, junctions and traction current sections.

The system shall be able to show geographically valid multiple bookings at similar or overlapping locations. See Appendix L, diagram view for and example of how this could be achieved using coloured lines to represent the extent or the bookings and a number to
The system shall show the geographic extent of a booking on a diagram type map.
The system shall make use of a London Underground map to show high level summaries of the number sof bookings on the network.
The system shall be able to visualise depot bookings. See Appendix L Ref-015 for an example of a depot visualisation used.
The configuration of the engineering trains required to support the work on the track needs to be defined. The configuration of the train will inform the planners of the length and make up of the train and could therefore affect the pathing of the train. Information described here will inform other departments who are required to load
The system must be able to add non LU trains and wagons to the for the purpose of pathing. I.e. GBRF trains that are required to be pathed.
The system shall hold a catalogue of the available wagons and locos that can be used to maintain and upgrade the underground network. Each item in the catalogue shall have at a minimum the following:
- Vehicle Unique Number
- Long Name
- Short Name
- Type (Loco, Wagon etc.)
- Length
- Laden Weight
- Unladen Weight
- Load Gauge
- Coupling requirements and incompatibilities
- Route restrictions
- Power Type (Diesel, Electric)
- Operational status (in service, out of service)
- CTC Start Date
- CTC End Date
- Planned maintenance dates

The system apply catalogue based rules to prevent users from requesting train formations that will not work.
The system shall hold a catalogue on pre-set standard train formations made up from the contents of the loco and wagon catalogue.
The system shall allow the user to add specific stock and or train formations as a favourite for ease of future use.
The system will allow a user to build a train from available locos and wagons.

The system shall calculate the total train length.

The system shall apply business rules on the total number of trains and or other vehicles that may operate on any given shift. The business rule should be configurable. e.g. current crewing limitations mean that only:
- 7 engineers trains and 2 tampers can run per shift
- only one train with the following wagons can run:
    - ELK (Electric Lifting crane)
    - Long welded rail train
    - Crane train.

The engineering trains that are required to support the work being carried out on the track required a train path to be allocated to ensure the train can arrive at site and depart the sit back to the depot with minimal or no impact to the work or passenger

The system shall constrain the overall trains route availability based on the most restrictive wagon or loco contained in the train formation.

The total length of a formed train may have restrictions on the underground network. Any train length restrictions are required to be taken into consideration when choosing valid train

A laden or unladed wagon may have different network restrictions and so the loading of a wagon needs to be taken into consideration when pathing trains.

The solution must record special restrictions relating to a wagon and therefore a train containing many wagons and locos. Such restrictions usually describe how the train should

The system shall record and time based restrictions that any loco or wagon has in travelling on the underground network.

The system shall have knowledge of all of the Wagons and units out of service due to maintenance. These units shall be made unavailable for planning and train pathing for the

The system shall know the following speeds of the formed train to enable a train path to be created:
- maximum speed
- average speed

The permanent and temporary speed limits for the underground network must be known to the system for the purposes of pathing trains.

The system shall highlight where changes to the TC switching times would be required because the introduction of engineering train paths where it has not been possible to keep

The system shall where possible make use of existing spare train paths and ensure that any engineering trains are pathed within the spare paths.

The system must accommodate train paths where engineering trains can be held at specific locations to enable no impact on the passenger services.

The system shall be able to animate/playback the engineering train paths required to support the track access.

The planning solution shall know about the existence of any work booked that affects the engineering train pathing for other work booked on the same day.

The planning system shall recalculate a new engineering train path if the existing path is impinged by work.

The planning solution must understand what are the available paths for each night Engineering Train paths from the Timetable Planning System.

The system shall allow permitted stock routes to be manually overridden if there is no valid permitted stock route. If this occurs the reason why the override has been carried out is to be recorded. This couple be because the stock is underground a route availability assessment and the approve document has not been entered in the system. Overriding this will allow trains to be pathed prior to the approval. The path cannot be published as

The system shall allow bespoke engineering paths to be created by the planner in addition to the available paths defined by the timetable system.
The system shall be able to calculate the maximum potential access time on site for the train as a result of its pathing.
The objective is to maximise the utilisation of a possession or closure by doing as much work as possible. Thereby reducing the congestion of engineering hours
The system shall describe the limits of the opportunity works as the limits of the existing possession or closure (there could be multiple possessions within a single closure).
The system shall define opportunity work candidates as:
- all bookings including those that have not started and have started.
- bookings that exist as a subset of the geographic limits of the possession(s) or closure
- bookings that exist as a superset of the geographic limits of the possession(s) or closure. These should be clearly distinguishable from the other types of candidates.
- bookings that exist within a user defined time window either side of the timescale designated for the possession(s) or closure.
- access plans with no associated bookings that may meet the criteria above.
(final field list to be decided in design phase)
The system shall present the candidate bookings as "opportunity works" for the selected possession(s)/closure. See Appendix L Ref-059 for an example of the existing Application
The system shall allow access requesters to subscribe to email alerts for planned possessions or closures based on a set of subscription criteria e.g. Underground line based;
The system shall be able to filter the opportunity works candidates in accordance with the criteria in req 190.
Protection resources are an integral part of the access planning process and so the required resourcing to support planned access is required to be captured.

The system shall be able to book protection resources for all types of access. See Appendix N for a list of the resource types used within the existing planning system.
(final field list to be decided in design phase)
The system shall understand the total cost of protection resources allocated to a booking and therefore the total cost of resources for a given project or programme.

The system shall use simple rules to limit the availability of the protection resource to support the protection of a worksite or possession. Examples of such rules are including a working time directive limit between consecutive jobs and a minimum requirement on
The system shall contain a catalogue of competencies, skills and familiarisation i.e. PWT-EH, Train master, Possession Controller. See Appendix N for examples of existing competencies used within the OGMS system.
The system shall be able to interface to existing competency based systems to obtain a record of the up to date competencies.

The system shall allow users to assign competence requirements to:
- a work request
- a possession plan
- a worksite.

The system shall hold a catalogue of protection staff containing at least the following information:
- Name
- Home Location
- Base availability
- Familiarisation of areas of the network
- History of shifts worked
- Performance management information
- Competences/skills held and expiry dates
- Availability (Training, holidays and sickness taken into consideration)
- History of work/areas
- Employer details
- Day rate (might vary based on competency used)

The system shall present to the users the location where the worksite that requires the protection resource resides (book on location).

The system shall help determine the distance from the worksite to the protection staff's home location.

The system will shall highlight when there will be shortages in resources required support planned work.

The system shall hold reports to aid the balancing of the work amongst the pool of resources.

The system shall allow protection staff to update their availability.

The system shall allow protection staff to accept or reject shifts.

Specialist equipment is sometimes required to support a piece of work. The availability of such resources should be able to be know when booking access to carry out the work within a worksite.

The system shall contain a catalogue of specialist equipment.

The system shall allow users to assign specialist equipment requirements to:
- a work request
- a possession plan
- a worksite.

The system will shall highlight when there will be shortages in specialist equipment required support planned work.

The system shall understand the total cost of the specialist equipment allocated to a booking and therefore the total cost of equipment for a given project or programme.

Work with in the access planning process is required to checked using a series of business rules to ascertain if multiple work types can exist at the same locations during the same timescales. Notifying both requesters and or planners of such

The solution shall clash check all work against the booked worksites and worksite protection limits.

If the solution finds no clash of worksite but a clash of worksite protection the system will inform the access planner via work flow so that a decision can be made at to if both works
The system shall check for clashes where the location of a worksite and/or protection limits overlap with another booking within the same time period.
The system shall check for clashes where the location of a possession or any booking within the possession overlaps with another booking within the same time period.
The system shall inform the requestor/owner of the booking of the extent to which the clash is occurring i.e. The worksite TCS's or protection site TCS's.
Where a booking is of access type non exclusive/non restrictive the process of managing the clash resolution will be left to the existing requester/booking owner.
The system will provide the existing requestor/owner of the booking with information on the overlapping/clashing booking in order that they can determine whether they can continue to work, cancel their work or contact the owner of the clashing work to coordinate their access.
The notification information presented to the existing requester will include and not be limited to the following:
- Booking Ref No.
- Requester Name
- Work Description
- Access Type
- Contact details
- Worksite limits
- Protection limits
- Date/Time for booking

When the new booking is a possession the notification information presented to the existing requester will include and not be limited to the following:
- Possession Ref No.
- Possession Owner (Business)
- Possession Planner (Access)
- Possession Description
- Access Type
- Contact details
- Possession limits
- Protection limits
- Date/Time for Possession

(final field list to be decided in design phase)
The system shall show clashed work visually to the existing requestor to aid them in understanding the impact of the clash.
The system shall transmit a clash message when a clash of two or more booking overlapping. Note some booking types will contain work that can overlap with other work
The system shall maintain a record of unacknowledged clashes in order that a clash notification is only raised once to the requester.
The system shall warn the person planning the access of any constraints or planning issues. i.e. getting a train to this location may prove difficult. The warnings can be ignored as they may not invalidate the booking only provide planning assistance during the planning
The system shall notify the booking owner of any cancellations to other bookings that previously existed along side their booking.
The system shall highlight traction current on/off clashes. In some cases work requires the TC to be switched off and in other cases the TC to be on. If this occurs for two bookings at the same overlapping locations and at the same time this should be highlighted to the

The resolution of valid overlapping work at the same locations and timeframe may require a number of approvals or checks to be taken by either the planners and or the requesters.

The system shall lock combinations of work so that no one can add other work or remove work without informing all parties. If work is required to be coordinated then all parties must agree any changes as work dependencies may exist.
The solution shall flag up where protection limits can be shared between two different track bookings.

Where a booking meets the initial criteria to sit along side and clash with another booking, both booking will exist within the system. In this example all parties involved in the overlapping work will be notified of the potential conflict and all the overlapping access bookings will exist and be planned to occur unless any of the requesters chooses to move
Where a booking exists within the system and another booking is made that clashes but meets the initial criteria to allow it to exist along side the other booking, the system shall instigate an approval work flow such that the original booking and potential new booking are both in a status that requires joint approval of each others bookings before any bookings are committed to the system. It is possible for any of the booking owners to remove their
Where a booking passes the initial criteria to sit along side and clash with another booking, both booking will exist within the system but will be set to a status "clashing" and require approval from the access planners before the booking is approved within the system. In this example all parties involved in the overlapping work will be notified of the potential conflict
The system shall allow the access planners to filter the booking clashes by the following and view them:
- Access Type
- Date Range
- Line
- Station Location

The system shall allow the access planners to approve/reject a booking clash.

The system shall log the time/date and planners name that approved the clash.

The system must prompt the access planner to enter a reason for the approval or rejection of the clash.

The system shall be able to clash an engineering train path against any planned bookings that may exist along the engineering train path.

The TC switching times may be required to be changed to accommodate engineering works that may need to run later thank planned and affect the timetable. Planning engineering trains to support the work being carried out may require the TC
The system shall record a catalogue of TC sections which enable the viewing of planned, actual and future TC switching times. See Appendix Lref-058 for a list of the minimum set of data required to define TC switching information.
The system shall allow planned changes to the core switching times to be entered in advance of their effective date.

The system shall import TC on and off switching times from RTS. See Appendix L Ref-029
Note the TCS base switching times are derived from the timetable generated by RTS, they include a number of empty paths before the last passenger train to accommodate possible
The system shall allow the users with the correct permissions to directly make temporary or permanent amendments to the traction current switching times.
The system shall keep and audit of any changes made to TC section times showing who and when the changes were made. See Appendix L Ref-011 for an example of the
The system shall highlight changes in TC times between different timetables.

The system shall highlight any planned work affected by TC switching time changes.

The system shall maintain a history of the TC switching times for all imported timetables.

The system shall be able to highlight any TC sections where a train is planned and there may be no TC power on.
The system shall make use of the effective timetable dates to ensure that any timetable extracted are applicable for a given calendar date.
The system shall enable the users with the correct level of permissions to make modifications to the timetable imported from RTS. When modifying the timetable a two step process should be adopted to ensure that the timetable modifications are checked and don't
Sometimes we are required to cancel engineering hours to accommodate operating the railway under operational conditions e.g. running new rolling stock tests under operational conditions.
The system will allow a Planner to indicate that specific TC sections will have no off time for given date/period.

The access within any planning system must be agreed by responsible individuals before the data can be used for operation purposes.
The system shall manage the access request submission timescales based on the access template type that adopts a time based workflow i.e. A closure defined will require greater that 222 days from when the work is supposed to occur to be submitted; bookings involving
The system shall allow the Access Planner to choose an option to override the submission timescales.
The system shall escalate any bookings that do not meet the approval timescales to the access manager via a workflow.
The goal of this function is to give the Access Team the correct set of tools to enable them to assure that the plans that are entered into the system are safe and workable when looked at as a whole. It is not expected that the system will be able to automatically mitigate all planning error. The system could highlight potential issues
The system shall be able to track commission and decommission rules for possessions. E.g. when a current section is physically spit the section need to be joined before the railway can be accepted back into operation. Any such rule shall be implemented as a
The System shall be able to record the lifecycle stages of possessions planning and use workflow to drive sequencing and task management.
The system shall allow users to place risk laden hotspots on a planned possession.
The system shall allow configurable hazard types to be assigned to hot spots.
The system shall allow resource requirements to be assigned against hazard types.
The system shall allow planners to identify the resources to mitigate the hazards against a

The system shall allow for assurance/approval workflow to move work from the planned to the published state and then to the operational state.
When engineering trains are pathed the system shall highlight:
- any missing late or early traction current switching times under the path of an engineering
- where the last train through a TC section changes mid way through the section e.g. due to a converging junction.
- where planned engineering trains paths pass through trains out stabled at a platform. See Appendix L Ref-013 for stabling locations report.
- where an engineers train path is not of sufficient gauge for the train
- where a planned reversing or stabling point is not long enough to accommodate the entire train.
- highlighting the work locations that are affected by the engineering train path
- any missing outward or return path for an engineering train travelling to a worksite or a possession
- any engineering train travelling to a worksite or a possession without working at site details.
When work is booked and planned the system shall highlight:
- where any exclusive or restrictive worksites overlaps with another planned worksite.
The system shall highlight cumulative risk where there are multiple worksites in a particular
When possessions are planned the system shall check that:
- there are no overlaps or gaps in the possession protection stages
- shifts align with possession protection stages - if this is a multi stage possession the stages ‘flow’ . (This relates to an engineering hours possession that would involve a depot, say to pass RRVs out of the depot at the start and finish of a possession into an adjacent possession – Stage 1 and 3 would cover larger areas and the middle stage 2 would cover the reduced area (excluding the depot)
- traction current sections within the possession align with the description of the possession area, and where more than one stage, reflect and growing or shrinkage of possession
- the protection area and method is sufficient to protect the worksites within the possession
- in the possession plan document that the switching arrangements are shown against each traction current section, including any revised late / early current
- where TC isolations are planned they start and finish
- that TC isolations are logical e.g. if a TC section is isolated by removing cables in a shift/stage, they are replaced in a subsequent shift /stage. Also if cables shown as being replaced in a stage, check that they were removed in an earlier shift/stage.
Publishing the planned and agreed access for operational staff to view is critical to maintaining and operating the underground.

The system shall be able deliver reports of a similar style contain all of the information contained within the following:
- NEPA (Appendix L Ref-001)
- 2 Week Look ahead EN (Appendix L Ref-003)
- Engineering Notice (Appendix L Ref-002)
- Possession Plan (Appendix L Ref-009)
- Stations Publications (Appendix L Ref-005, Ref-006, Ref-007, Ref-008).

(final report style, content and layout for initial go-live reports to be decided in design phase)

The system shall allow the creation of new reports using data contained within the Access
The system shall allow the modification of existing report within the Access Planning
The system shall allow users to share reports or maintain a private repository.
The system shall be capable of being integrated with TfL reporting and Business
The system should provide APIs to allow booking, planning and possession information to be shared with other applications in real time.
The ability to report on all of the data within the access planning system will give the access planners and requesters the flexibility to perform analysis on the data within the system and produce report that may be of use when carrying out their roles.
The solution shall be designed such that the data available for reporting can be 'tuned' to specific roles or organisations within the system. This will enable sensitive information such as cost to be hidden from certain users of the system.
The system shall be able to produce planning reports containing the same information as published using SABRE information. See Appendix L Ref-043 to Ref-048 for examples of existing reports produce to aid with the planning process. Appendix K describes more detail about the content of the reports.
The system shall be able to reproduce reports with historic information, thus maintaining a copy of all historic base data to reproduce the reports.
The system shall be able to produce a report showing the events on a geographic diagram.
When the work requester is intending to carryout work on or around the railway, he/she will confirm that they will be requiring the booked access. When confirming access opportunity the requester must state the precise timescales for the work.
The system interface with the Access Control System to provide information such as:
- Track or station booking
- Hazards for booking
- TCS for track booking
- Station locations
- Work team provider
- Work details
- Access booking type
- Booking reference number
- Validity time period (dates and shifts)
- Planned access and egress points (station, depot etc.)

This list is not exhaustive.
(final field list to be decided in design phase)

The system shall be able to capture the following information from the access control system:
- Book on time
- Book off time
- Work party details
- TCS utilised for track bookings
- Actual access and egress points
- Access allowed/refused
- Refusal reason
- Station representative processing booking

This list is not exhaustive.
The system shall allow System Admin to create, update and delete reference data.
The system shall manage the referential integrity of the reference data and ensure that deleted data is still made available for historic reports.
The system shall be enable System Admin role to create and update/design e-form and its
The system shall enable System Admin to be able to manage the creation of business rules. A business rule would consist of one or more conditions, actions based on those conditions and allow for specific exceptions. See the Appendix H.
The system shall be able to allow any business rule to be constructed with simple logic
The system shall allow the System Admin to apply a selection of business rules to an e-
The Access Plan Approver (Access Planner) shall be able to select the relevant e-forms (from a library), apply the relevant business rule to the e-form and make it available to
The system shall allow the System Admin role to allocate e-forms to a e-form library.
The system shall allow the System Admin to put the business rules into a business rule
Appendix L Ref-049 contains a list field that are currently present on the access request form. The fields have been categorised (drop down, selection boxes, multi field selection fields with business rules applied).

Data structure requirements define many of the critical objects and classes on data that is required to be present with the access planning system.

The solution shall assign work within a worksite. Multiple works can occur in a single work
The solution shall associate work site protection limits to a worksite. These protection limits may not have any work contained within them but solely be used to protect the workers and
The solution shall associate an access booking as the contents of a worksite and protection
The system shall highlight any work site lying within the protection area for a Possession or Closure. See Appendix Q for an example diagram of how access planning limits will work.
Each piece of work with a worksite shall have its own access type classification/flag based on whether the work restricts others from the type of work they will undertake or prevents others from doing any work within the area. The current classifications are:
- Exclusive
- Restrictive
- Non Exclusive/Non Restrictive.

Where another booking contains a worksite with overlapping timescales and location the requester of the requested of the new piece of work must be able to assure themselves that they can co-exist within the same worksite as the restrictive booking. (final category list to
The system shall store details of areas/zones and rooms within stations.

The system shall store details of critical assets within stations such as escalators, lifts (See Appendix L Ref-024, Ref-025 & Ref-026 for station plans and station zones)

The system shall maintain relationships between objects. See Appendix G class diagram for examples of the main data types and their relationships.
The system can include the following in a booking:
- Track Worksite(s)
- Access and Egress points
- Station Worksite(s)
- Associated Engineering Trains
- Associated Specialist Equipment Resources
- Associated Protection Resources
- Train Pathing for required engineering trains

The system shall contains geography to describe both track, depot and stations within the
The system requires to understand the following information for track:
- Track layout
    - Actual running rails/actual current rails
    - Rail Type
    - Gradients
    - Tunnel Clearance/Gauge
    - Bridges/over structures/under passes
    - Sidings/platforms/Reversing Point Lengths
- Signal and Track Circuit Layout
    - Track Circuits
    - Fixed signalling assets such as
        - headway/marker boards
        - Colour light signals
        - shunt signals
    - Points and crossings
- Traction Current Supply Layout
    - Traction current electrical section Sub station feeding arrangements. See Appendix X.
    - Traction current section switches and changeover switches
    - Temporary section gap cut to facilitate temporary altered current arrangements for a possession.
    - Traction current sections associated for switching purposes (e.g. TC rail positions contain a staggered gap)
- Access Points
    - Gates
        - Width
        - Suitability for foot or vehicle access
    - Vent shafts and other intervention points

The system requires to understand the following information for depots. See Req 253 plus the following additional information:

- Depot Road Name/Number/Area Type
- Electrified/Non electrified with TC data as main line.
- Road Type
    - Lifting
    - Pit

(final list to be decided in design phase)

The system requires to understand enough topographical data for stations to facilitate the booking of:

- Rooms/corridors/open areas/platforms
- Lifts and escalators
- Secure rooms (machine rooms, electrical rooms, signalling rooms, ticket office)
- Disused areas
- Vent shafts
- Stairs
- External areas.

The system shall be able to logically group any of the station information into zones.
The system shall be able to record access planning information based on:
- historical
- current
- future

geography defined within the system.
The system shall provide the published TC switching times to the Access Control system.

The system shall provide the generic call back times associated with the published TC switching times to the Access Control system.
The system shall provide the amended TC switching times to the Access Control system.

The system shall provide the "split" TC sections to the Access Control system. This may include showing the feeds either side of a split. Where there are multiple splits on a single
The system shall provide the Access Control System will a list of the hazards applicable to an access booking.
The system shall provide verified and suitable for operational working bookings to the Access Control system.
The system shall provide the call back times for a specific booking if different from the generic call back time for the TC sections that work is planned to take place on to the
The system shall import the published last train information from Railway Timetable System (RTS) (Appendix L Ref-030).
The system shall import current (and future when they are available) Traction Current switching times from the Railway Timetabling System (RTS) (Appendix L Ref-029).
The system shall import the engineering train, available paths information from the Railway Timetabling System (RTS) (Appendix L Ref-031).
The system shall be able to use the information contained within the Engineering Train Route Availability document (Appendix Ref-018).

The system shall provide the following approved track booking information to the CTAC system (Access Planning System):
-Unique booking ID
-Booking location(s)
-Description of work
-Work Team Provider
-Work Team Provider Contact Number
-Location of Hazards, such as specified areas, engineers current areas and possessions
-published and amended TC switching times
(final list to be decided in design phase)
The system shall provide the following approved station booking information to the Permit Access system (Access Control):
-Unique booking ID
-Work Team Provider
-Accountable Manager Name
-Accountable Manager Phone Number
-Category of Work
-Description of work
-Special Arrangements
-Start Date/Time
-End Date/Time
-Line
-Station
-Status
(final list to be decided in design phase)
The system shall make the access planning possessions information available to the OGMS database.

The system shall import all of the information listed in Requirement 253 from the TfL GIS. See Appendix O.
The system shall be able to import the station diagrams (see Appendix L Ref-024, Ref-025 & Ref-026) . The diagrams contain the following information:
- Station zones
- Critical rooms
- Station layers
- Critical assets (e.g. Lifts and escalators)
...
Have you utilised interfaces between your solution and third party systems? Please provide a brief description of the type of interface. If your solution provides other interfaces

				Metho
Importance	**URS Reference**	**Compliance Level (Fully/Partial/Non Compliant)**	**Out of the box (Y/N)**	**Configuration Required (Y/N)**
Must Have				
Must Have				
Must Have				
Must Have				
Must Have				
Should Have				
Must Have				
Must Have				
Must Have				
Must Have				

Must Have		[redacted]
Must Have	Appendix L Ref-016	[redacted]
Should Have		[redacted]
Should Have	Appendix F2.2	[redacted]
Must Have		[redacted]
Should Have		[redacted]
Must Have		[redacted]
Must Have		[redacted]

Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have	Appendix L Ref-017	
Must Have		
Must Have	Appendix L Ref-057	
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		

Must Have	Appendix P	[redacted]
Must Have	Appendix P Appendix L Ref-039	
Must Have		
Must Have	Appendix L Ref-039	

Must Have		[redacted]
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have	Appendix L Ref-017, Appendix L Ref-057	
Must Have		

Must Have		[redacted]
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must have		
Must Have		
Must Have		
Must Have		
Must Have		
Should Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have	Appendix L Ref-023, Ref-027, Ref-028, Ref-055	
Must Have	Appendix F	
Must Have		

Must Have		[redacted]
Must Have		
Must Have		
Must Have	Appendix L Ref-052, Ref-024, Ref-025, Ref-026	
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Should Have	Appendix H	
Must Have		
Must Have		

Must Have

Must Have

Must Have Appendix P

Must Have	Appendix P	[redacted]
Must Have	Appendix A	
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have Must Have Must Have Must Have		
Must Have Must Have		
Must Have Should Have		

Should Have

Must Have

Must Have

Should Have

Should Have

Should Have

Should Have

Should Have

Should Have

Must Have

Must Have

Must Have
Must Have Appendix I

Must Have

Must Have

Must Have
Must have

Must Have

Should Have

Must Have

Should Have

Should Have

Must Have
Must Have
Must Have
Must Have

Must Have
Must Have

Must Have
Must Have

Must Have		[redacted]
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have	Appendix L Ref-010, Ref-012	
Must Have	Appendix L Ref-041	
Should Have		
Must Have		
Should Have		
Should Have		
Must have		
Should Have	Appendix L Ref-060	
Should Have		

Should Have	
Should Have	
Should Have	
Should Have	
Should Have	
Should Have	
Should Have	
Must Have	
Should Have	Appendix F, Appendix J
Must Have	Appendix F
Must Have	Appendix F
Must Have	Appendix F
Must Have	Appendix F
Must Have	Appendix F
Must Have	Appendix F
Should Have	Appendix F
Must Have	Appendix F
Must Have	Appendix F
Must Have	Appendix F
Must Have	Appendix F
Must Have	Appendix F

Must Have	Appendix F	[redacted]
Must Have	Appendix F	
Must Have	Appendix F	
Must Have	Appendix L Ref-015	
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		

Must Have	Appendix L Ref-056	[redacted]
Must Have	Appendix L Ref-020	
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Should Have		
Must Have		
Must Have		
Must Have		
Must Have		

Must Have		[redacted]
Must Have		
Must Have		
Must Have		
Must Have	Appendix L Ref-059	
Must Have		
Must Have		
Must Have	Appendix N	
Must Have		
Must Have		
Must have	Appendix N	
Should Have		
Must have		

Must have

Must Have

Should Have

Must have

Must have

Must have

Must have

Must have

Must have

Must have

Must have

Must have

Must Have

Must Have

Must Have

Must Have

Must Have

Must Have

Must Have

Must Have

Must Have

Must Have

Must Have

Should Have

Must Have

Should Have

Must Have

Must Have

Must Have

Must Have		
Must Have		
Must Have		
Should Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have	Appendix L Ref-058	
Must Have		

Must Have	Appendix L Ref-029	[redacted]
Must Have		
Must Have	Appendix L Ref-011	
Must Have		
Must Have		
Must Have		
Must Have	Appendix L Ref-029	
Must Have		
Must Have		
Must Have		
Must Have	Appendix H Example 14.	
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		

Must Have		[redacted]
Must Have	Appendix l Ref-013	
Must Have		
Must Have		
Must Have		

Must Have	Appendix L Ref-001, Appendix L Ref-003, Appendix L Ref-002, Appendix L Ref-009, Appendix L Ref-005, Appendix L Ref-006, Appendix L Ref-007, Appendix L Ref-008, Appendix L Ref-004	[redacted]
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have	Appendix L Ref-043 to Ref-048, Appendix K	
Must Have		
Must Have		
Must Have		

Must Have		[redacted]
Must Have		
Must Have		
Must Have		
Must Have		
Must Have	Appendix H	
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have	Appendix L Ref-049	
Must Have	Appendix G	
Must Have		
Must Have		
Must Have	Appendix Q	
Must Have	Appendix H	
Must Have		

Must Have	Appendix L Ref-024, Appendix L Ref-025, Appendix L Ref-026	[redacted]
Must Have	Appendix G	
Must Have		
Must Have		
Must Have	Appendix L Ref-023, Ref-027, Ref-028, Ref-055	

Must Have		[redacted]
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have		
Must Have	Appendix L Ref-030	
Must Have	Appendix L Ref-029	
Must Have	Appendix L Ref-031	
Must Have	Appendix L Ref-018	

Must Have		[redacted]
Must Have		
Must Have		
Must Have	Appendix O	
Must Have	Appendix L Ref-024, Appendix L Ref-025, Appendix L Ref-026	
Must Have		

Tender Responses

d of Delivery		
Custom Development (Y/N)	Integration Development (Y/N)	Met Requirement Comments

Un-met Requirement Comments

APPENDIX F

Access Planning URS Non-Functional

TfL Access Planning Non

Tender Category	Req ID	Category	Requirement Name
Application Support	NFR072	Application Support	Support Window
Application Support	NFR073	Support & Availability	Planned downtime/maintenance windows
Application Support	NFR117	Support & Availability	Availability – Support Hours
Application Support	NFR074	Disaster Recovery (DR)	Server resilience
Application Support	NFR075	Disaster Recovery (DR)	DR automation
Application Support	NFR076	Disaster Recovery (DR)	Recovery Point Objective (RPO)

Application Support	NFR077	Disaster Recovery (DR)	Recovery Time Objective (RTO)
Application Support	NFR078	Application Support	Data Recovery
Application Support	NFR079	Application Support	Maintenance
Application Support	NFR081	Application Support	ITIL Alignment
Application Support	NFR082	Service Desk Integration	Support Process
Application Support	NFR083	System Administration	Maintenance
Application Support	NFR085	System Administration	
Application Support	NFR086	SLA’s and Service Credits	Availability

Application Support	NFR087	SLA’s and Service Credits	Service Levels
Application Support	NFR089	Service Performance and Management information reporting	Service Model
Application Support	NFR091	Service Performance and Management information reporting	Management Reporting

Application Support	NFR092	Service Performance and Management information reporting	Service Reports
Application Support	NFR093	Service Performance and Management information reporting	Scheduled Meetings
Delivery Capability	NFR030	Development Capabilities	Skills
Delivery Capability	NFR031	Development Capabilities	Development Location
Delivery Capability	NFR032	Development Capabilities	External support / relationships
Delivery Capability	NFR033	Development Capabilities	Skill Development
Delivery Capability	NFR034	Implementation Capabilities	Skills
Delivery Capability	NFR035	Implementation Capabilities	Breadth of capability
Delivery Capability	NFR036	Implementation Capabilities	External support / relationships
Delivery Capability	NFR037	Implementation Capabilities	Skill Development
Delivery Capability	NFR038	Project Management	Project size
Delivery Capability	NFR039	Project Management	Project Structure
Delivery Capability	NFR040	Project Management	Experience
Delivery Capability	NFR041	Project Management	Communications
Integration and Delivery	NFR058	Data Migration	Data Migration
Integration and Delivery	NFR059	Data Migration	Tools
Integration and Delivery	NFR060	Data Migration	Planning
Integration and Delivery	NFR061	Data Migration	Challenges
Integration and Delivery	NFR062	Integration	Integration
Integration and Delivery	NFR063	Integration	Tools
Integration and Delivery	NFR064	Integration	Planning
Integration and Delivery	NFR065	Integration	Challenges
Integration and Delivery	NFR066	Data Presentation	Tools

Integration and Delivery	NFR067	Data Presentation	Planning
Integration and Delivery	NFR068	Data Presentation	Challenges
Methodology, Standards and Approach	NFR042	Delivery Methodology	Implementation
Methodology, Standards and Approach	NFR043	Delivery Methodology	Artefact Production
Methodology, Standards and Approach	NFR044	Delivery Methodology	Development
Methodology, Standards and Approach	NFR045	Delivery Methodology	Testing
Methodology, Standards and Approach	NFR046	Delivery Methodology	Design
Methodology, Standards and Approach	NFR047	Delivery Methodology	Knowledge Transfer
Methodology, Standards and Approach	NFR048	Delivery Methodology	Development Support
Methodology, Standards and Approach	NFR049	Quality Approach	Methodology
Methodology, Standards and Approach	NFR050	Quality Approach	Governance
Methodology, Standards and Approach	NFR051	Quality Approach	Quality
Methodology, Standards and Approach	NFR052	Project Plan	Plan Communication
Methodology, Standards and Approach	NFR053	Project Plan	Content
Methodology, Standards and Approach	NFR054	Project Plan	Frequency
Methodology, Standards and Approach	NFR055	Project Plan	Ownership
Methodology, Standards and Approach	NFR056	Project Plan	Variance and change
Methodology, Standards and Approach	NFR057	Discovery	Approach
Solution Design	NFR001	Support & Availability	Health monitoring
Solution Design	NFR002	Scalability & Flexibility	Growth metrics

Solution Design	NFR003	Scalability & Flexibility	Change cases
Solution Design	NFR004	Scalability & Flexibility	Technology
Solution Design	NFR005	Data connectivity & system interfaces	System Interfaces
Solution Design	NFR006	Volumetrics	User base

Solution Design	NFR007	Volumetrics	Number of transactions
Solution Design	NFR008	Infrastructure & Architecture	Dedicated training environment
Solution Design	NFR009	Infrastructure & Architecture	Dedicated testing environment
Solution Design	NFR010	Infrastructure & Architecture	Environments
Solution Design	NFR011	Infrastructure & Architecture	Desktop configuration
Solution Design	NFR012	Infrastructure & Architecture	Desktop configuration
Solution Design	NFR013	Infrastructure & Architecture	Connectivity
Solution Design	NFR014	Infrastructure & Architecture	Network
Solution Design	NFR015	Security	User Authentication
Solution Design	NFR016	Security	Role-based access permission
Solution Design	NFR017	Security	Multi-level access privilege
Solution Design	NFR018	Security	Switching between roles
Solution Design	NFR019	Compliance	TfL Architecture Standard

Solution Design	NFR020	Performance	Transaction response time
Solution Design	NFR021	Data Management	Data migration
Solution Design	NFR022	Data Management	Data disposal
Solution Design	NFR023	Auditing	Auditing database records
Solution Design	NFR024	Auditing	Users' audit trail
Solution Design	NFR025	Usability	On-line help
Solution Design	NFR026	Usability	Intuitiveness
Solution Design	NFR027	Usability	Error messages
Solution Design	NFR028	Usability	Clear navigation
Solution Design	NFR029	Usability	Role-based User Interface
Solution Design	NFR100	Value Added	Value Added
Training	NFR069	Training	Training Capabilities
Training	NFR070	Training	Training Approach
Training	NFR071	Training	TfL Enablement

Application Support	NFR101	Service Management	Warranty
Application Support	NFR102	Service Management	Incident Investigation
Application Support	NFR103	Service Management	Software Licencing
Application Support	NFR104	Service Management	System Updates
Application Support	NFR105	Service Management	Roadmaps
Application Support	NFR106	Service Management	Support Desk
Application Support	NFR107	Service Management	Change Management Process
Application Support	NFR108	Service Management	Release Management
Application Support	NFR109	Service Management	Major Incidents
Application Support	NFR110	Service Management	Problem Management
Application Support	NFR111	Service Management	Continuity Plans
Application Support	NFR112	Service Management	Technical Support Material
Application Support	NFR113	Service Management	Configuration of system
Solution Design	NFR114	Infrastructure & Architecture	System Monitoring
Solution Design	NFR115	Infrastructure & Architecture	Security
Solution Design	NFR116	Infrastructure & Architecture	Compliance

Functional Requirements

Requirement Description

The system shall be available, function and perform as specified during the Access Planning and Control operational and critical service hours: 24 hours a day 7 days a week.
The critical hours of operation can be split into two daily timeslots:
• Core planning functions 7am to 7pm
• Interfacing with access control 7pm to 7am.

• Planned downtime shall preferably occur within the window of: 07:00 – 12:00 hours Saturday to Sunday.
• Changes to the system shall be, where possible, avoided after 12:00 hours to give sufficient time for unplanned problems with deployment and sufficient time to restore the service prior to the start of engineering hours and track access bookings for that given night.
• The system should not, during its hours of operation, incur unplanned downtime more than
The system will require support 24 hours per day, 7 days a week. The supplier will need to cover core hours during the 365 days annually. The Severity Level will be agreed with the Supplier at contract finalisation.

Severity Level 1:
Response time of 30 minutes. Target: 98% of Sev 1 incidents to be resolved in 2 hours.

Severity Level 2:
Response time of 30 minutes. Target: 98% of Sev 2 incidents to be resolved in 4 hours.

Severity Level 3:
Response time of 30 minutes. Target: 98% of Sev 3 incidents to be resolved in 8 hours.

If bidders are unable to meet this requirement they are asked to suggest alternative support hours along with their rationale for proposing these support times
The system shall be designed and built to ensure a high level of resilience of the servers – Disaster Recovery, Production, Testing and Database.
The level of resilience built into the system shall ensure the realisation of the RTO and RPO specified in this document.
Bidder notes:
Bidders must detail the disaster recovery requirements and capabilities of the solution. For non-SaaS based components, a proposed solution architecture that outlines the Bidder's recommended solution architecture, incorporating DR, should be provided; including technical requirements (e.g. database redundancy approaches), DR related service
Geographic resilience shall be built to ensure there is no single failure point associated with a geographic location.
Recovery Point Objective represents the maximum amount of data that it is permissible for the core system to lose as a result of system-wide operational failures (i.e. failures that are not classified as a disaster where an entire data centre is made unavailable).
The data loss target for the solution should be 30 mins. Any failed data transfers that occur during system failure shall be retransmitted.

Recovery Time Objective represents the maximum amount of time it should take for the system to be restored to an operational state for system-wide operational failures (i.e. failures that aren't classified as a disaster where an entire data centre is made unavailable). For a solution option delivering the availability target of 99.8%, the maximum recovery time should be no more than:

• 2 hours for core access planning functions

• 30 mins for access control interface functions (see Appendix O Req IDs 150 to 156 and

Data within the system should be recoverable to a specified point in time at differing levels of granularity (e.g. for a particular user, for a particular change).

Additional bidder notes:

Bidders should outline how their proposed solution supports this requirement, what level of granularity of data restore is possible, what process would be utilised to initiate and perform the restore and the implications of these.

The solution should not be impacted by any systems maintenance or management activities such as software or hardware upgrades without being agreed prior with Transport for London and London Underground. Any planned downtime must be agreed between the parties prior to implementation.

Additional bidder notes:

Bidders should specify how the proposed solution is able to meet this requirement what would be required to meet the requirement.

Bidders are asked to give an overview of their current working practices that are in line with ITIL v3 guidelines.

Answer should be no more than 250 words.

Bidding companies should respond with their suggested internal support process together with the details of their supporting infrastructure (e.g. help desk, service hours, number of staff etc.). Please also state for each element listed, if the element is existing and proven, or not.

If it is an existing process the response should also include the volumes of calls currently processed.

Bidders are asked to describe how they will carry out scheduled maintenance. This should include details of the maintenance activities, timescales, frequency and any other relevant information.

Answer should be no more than 250 words.

The service needs to include:

- Major upgrades with at least one major upgrade during the life of the contract including any associated costs by the supplier.
- Minor upgrades as a result of bug fixes or minor enhancement requested by other customers.

Bidders should confirm acceptance of this and ensure that any associated costs are

The solution must be designed and implemented to be available 99.8% of the time during its hours of operation. Availability target is calculated from supported hours of operation (excluding agreed scheduled downtime).

Bidding companies should confirm that they can comply with the Service Level Requirements within the Contract or, if appropriate, suggest alternatives. In order for greater clarity bidders should reply to this question by completing a table with the headings below for each requirement:

1. Requirement
2. Partially Compliant
3. Non-compliant
4. Reason for partial or non compliance
5. Alternative solution

Answer should be no more than 500 words

Prior to take on of service into support, TfL require completion of a TfL Service Model document. The bidder shall be required to enter into discussions to assist drafting and agreeing this Service Model document.

This document shall describe:

- The final service solution, support organisation, support responsibilities and the relevant support processes of parties involved in the delivery of the service.
- How the service provider will interact at an operational level with TfL's existing service providers (internal and external) for the management of incidents, requests, releases and changes.
- How all support parties (TfL, bidder and other third parties) will deliver services to support the final solution.

The Service Model is to be completed before service is handed over and made operational. Bidders are asked to confirm their acceptance of this requirement.

If the proposed solution includes any local client software then TfL will require a range of support material to be produced as part of service take on to live support, these include documents such as:

- Operations Manual;
- FAQs;
- Known Errors (defect log);
- Service Catalogue entries;
- First Line Support Troubleshooting Guide;

Bidders shall provide detailed management reports in order to ascertain service levels achieved which allow service costs to be calculated and managed. The reports shall be provided electronically to TfL on a monthly basis. Each report shall encapsulate the following:

- Availability statistics for that period for the Service, with accompanying commentary;
- Incident and problem statistics for that period for the Service, with accompanying commentary;
- Detailed breakdown of incidents and problem tickets, showing the description, time logged, the time responded to, the time resolved and whether the SLA was achieved;
- Explanations for any breach of service target and actions taken to mitigate risk;
- Trend analysis on types of failures;
- Service credit details;
- Pending/future actions;
- Recommendations for continual service improvement.

Bidders are asked to outline their approach to reporting and confirm whether the above

Bidders shall produce ad hoc service reports if requested by TfL. These will normally be following exceptional events or security breaches that require further investigation. Bidders are asked to describe how they would manage any requests for ad hoc reports, including their method of delivery.
Answer should be no more than 250 words
The bidder's Account Manager shall meet with representatives of TfL IM Supplier Performance & Assurance and any other relevant TfL team as agreed with each other and at a location to be specified by TfL. Topics to be covered within the service review meeting will include:

- Bidder performance against SLAs
- Any service issues and incidents not met within SLA, and proposed remedial work
- All security incidents or observations (irrespective of source or responsibility)
- Any proposed changes to the service
- Product roadmaps
- Invoicing/payment
- Any other issues or opportunities

Bidders are asked to outline their approach to service review meetings, and describe how they would undertake them with TfL
Please describe the extent of your development capability (skills, number of staff, grades, structure etc.)
Where does your development capability sit (off-shore, on-shore, internal, partner etc.)?

Outline formal relationship and contracts to provide support and escalation in the event that development challenges are experienced (both technical and resource shortfalls)
How do you ensure that your development staffs' skills are maintained and current?

Please describe the extent of your implementation capability (skills, number of staff, grades, structure etc.)
Describe the extent that your design capability extends to (infrastructure, network, application, development, support etc.)
Outline formal relationship and contracts to provide support and escalation in the event that development challenges are experience (both technical and resource shortfalls)
How do you ensure that your implementation staffs' skills are maintained and current?

What size of Project team would you use for this delivery?
How would the Project team be structured? Please include roles responsibilities and deliverables that each team member would be accountable for.
What experience does the Project team have with working with customers within the Public Sector, are there particular approaches or methodologies that you would find more
What methods of communication would the Project team use internally and externally?
What content would be communicated and with what frequency.
Based on experience and your knowledge of the TfL requirements what (if any) data
What standard tools and processes would you use for data migration?
How would you typically plan and validate a data migration exercise
What are the principal challenges that you anticipate within the data migration domain?
Based on experience and your knowledge of the TfL requirements what (if any) integration
What standard tools and processes would you use for integration?
How would you typically plan and validate a system integration
What are the principal challenges that you anticipate around integration
How does your system present data to other applications?

What standard design and deployment approaches do you take for exposing data to third
What are the principal challenges that you anticipate with presenting data to other systems
Provide a detailed overview of implementation methodology.

What typical design artefacts would you expect to deliver?

Provide an outline of your development approach and methodology.

Provide a detailed overview of your testing methodology and approach (for development and implementation).
Please describe the design governance approach that you undertake, outlining the clients responsibility within this.
How do you transfer knowledge associated with development and implementation to ensure that support can be undertaken by the client.
What support is provided for client development teams?

What project methodology would the team use? If not a standard recognised methodology please describe your internal methodology or the delivery method that you would adopt.
What internal and external governance processes does your company adhere too, Please include any reference to gated delivery processes.
How does your organisation ensure quality planning, quality control and quality assurance?

How would the Project plan be communicated with TfL

What information would be included in the Plan?

How often would the plan be communicated with TfL?

Who in your organisation would own the Project Plan?

How would variances to the baselined and agreed plan be handled?

How will your company approach the discovery phase including the type and level of engagement required from TfL.. In the light of requirement set in this ITT what measures will your organisation take to ensure that the requirement set is accommodated, documented and any exceptions catered for. How long do you anticipate (elapsed time) that the discovery phase will take? What outputs from discovery will you produce and how will

- The system shall be constantly monitored for operational readiness.
- The system shall automatically generate an alert for the support team whenever any of its component experiences a down-time.

1 User base: it is assumed the number of users of the system will remain relatively stable over the coming years.
2 Transactions: it is assumed, for now, that the volume of transactions will remain stable over the coming years. However an increase in the number of engineering works due to the proposed introduction of weekend night service sometime in September of 2015 may change this assumption.
3 Data: the volume of data could potentially grow in the coming years, if for example there is an increase in the number of train services.

It is expected that the system will evolve in various ways over the coming years, to support changes in business processes as well as cater for new business requirements.
The implementation of this upgrade or replacement, therefore, needs to be sufficiently flexible to accommodate the following needs:
1 Interface with non-TfL systems/networks;
2 Interface with other TfL systems;
3 Changes to TfL technological road map;
4 Additional users accessing different parts of the system

The chosen technology should not be end of life within the life of the contract.

The system shall be designed and built with the functions/features that will enable it to interface to the following systems:
• Access Control System(s)
    o Permissioning System – Tender in process
    o CTAC – TfL bespoke system maintained by CSC
    o Permit Access System – TfL bespoke system maintained by internal IM
• Railway Timetable System (RTS) - TfL bespoke system maintained by BAE
• CART - TfL bespoke system maintained by CMC
• Power SCADA System - Tender in process
• OGMS - TfL bespoke system maintained LU Access Planning Department
• TfL Corporate Geographic Information System (GIS) Supplied by Intergraph. See Appendix Q for a more detailed description of the TfL GIS system.
See Appendix Q Phase Type “Interfaces” and Req ID 023, 024, 025, 027, 028, 036, 037
• The total number of users of the Access Planning System are defined below:

User Type	Total Number of Authorised Users	Number of Concurrent Users
External Users	2000 users will be using the system in a typical evening/night	
External Requesters	500	200
Internal Planners	141	74
Configuration Manager	3	1
Assurance/Approval Users	20	10

External Users: These are users who will be using information from the access planning system to book onto stations and the track during a given evening or night. The users will normally interact with the access control system(s) and the access control system(s) will

The following volumes of data are expected to be in the system:

Data Type	Number of records
Requests requiring no further planning	2000 per year
Requests requiring a closure:	
Track - 240	
Stations - 233	
Depots & Sidings - 1210	
Passenger Stock Outstabling 100	2000 per year
Requests requiring a possession plan	250 per year
Requests requiring further planning and approval (Non closures and not possession but is Exc or Res)	1000 per year
Programmes	200
Projects	2000
Access Plans submitted	2-5 per project
Train paths required	100 per week

A dedicated training environment/facility shall be provided for Access Planning during the implementation phase of the project.
A dedicated testing environment/facility shall be provided for Access Planning during the implementation phase of the project.
A shared testing and training environment/facility shall be provided for Access Planning post implementation an go live of the project.
The system's desktop environment shall be designed and configured to enable users to use only a single desktop machine for both Access Planning and general TfL applications.
The systems desktop configuration shall be compliant with the TfL standard desktop build.

Users of the Access Planning System should be able to interact with the system in the following ways:
• External users – directly into the system when not connected directly to the TfL network or without using a TfL desktop.
• Mobile users – completing simple work requests and submitting forms can be carried out using a mobile device such as a smart phone or tablet.
The main access planning users will be located in the same office location connected to the main TfL network.
• The system shall authenticate the permission rights of anyone accessing it. At the minimum, users shall be required to log in to the system using a username and password.
• The preferred authentication mechanism shall be Single Sign-On for internal staff.

The system must be able to support roles-based access permission.

The system shall have the capability to provide multiple tiers of access privilege to certain users.
Users with multi-level access privilege shall be able to switch between roles without having to log out and then log back in to the system (roles to be assigned to a person).
Any part of the solution that will be deployed onto the TfL estate must comply TfL standards.

The following components of the system shall operate and return results in the following timescales:

Function/Component	Response Time No more than
Clash checking for an individual item	2 seconds
Response time for form or page to be presented an available to a user	2-3 seconds
Simple tabular reports to be generated	30 seconds
Complex formatted reports (such as NEPA)	60 seconds
Optimisation of plans and train pathing functions	180 seconds

Some of the existing data within the SABRE and Possessions Database system will be required to be migrated to the new Access Planning System.

- Protection Staff Resources– 450
- Master Geographic information
- TCS (Traction Current Section) Codes - 372
- LCS Codes -1734
- SID Code (Room Codes) – 32000
- SABRE bookings already in existing systems - 2000

Data disposal processes and procedures should be in place to ensure an orderly disposal of historical and unused data from all the system's components, including production database and all backup and Disaster Recovery media. Documented procedures describing

1. The application must maintain an audit trail of changes made to all database records and provide facilities to enable system administrators to view audit logs.
2. The system must record the date and time data is created, modified or deleted, the user performing the action and the value attributed to the data before and after the change was performed.

The system shall maintain an audit trail outlining:

- Who has made changes to data and when; and
- Who has made changes to the application's configuration and when.

The system's developer or supplier shall ensure users have access to on-line help.
The system shall display messages understandable to the user in the event of errors and instruct the user on what to do given the context of the error.
The system shall provide clear information indicating the cause of any errors resulting from user, transaction or system failures. All fields shall have appropriate data validation to
The system's user Interface should provide clear and unambiguous navigation whereby users are presented with clear paths to all parts of the application as well as an indication of
The system shall have the capability to support role-based customisations of the User Interface in terms of the data displayed and the functions made available as such that users, at any given time, are presented with an Interface that is contextual to the role they
Please explain in detail how your solution might add value to our overall Work planning, Access Planning, Access Control and Work Progress Reporting end to end process utilising other functions or modules of your system that would be available to TfL. It would be useful to understand how your organisation has previously suggested additional functionality to
Please explain in detail the training capabilities that your organisation can provide. Include standard and customised material that may be available, any computer based training or web-based offerings. It would be useful to understand how your organisation has
Considering your understanding of the requirements and the different roles (admin/supervisor/general user/planner etc.) Do you have a recommended approach for
What facilities/materials does your organisation offer to enable TfL Trainers to adopt the

TfL requires a minimum period of warranty of four weeks on initial Go Live to ensure that
The bidder shall describe their experience and approach to accessing the customer estate for the purposes of service delivery and support.
E.g. for incident investigation and fixing; and for changes.

The bidder will adhere to TfL Software Licencing Standard. Bidders are required to ensure that all software licence documentation and physical media are sent to TfL's Licence Management Team. See "Licence Requirements for TfL.doc" contained within the attached
TfL require the system to be correctly patched and updated to ensure that system is supportable by the supplier and our internal TfL teams and 3rd parties.
Bidders are required to provide product roadmaps for all components within the solution.
TfL require that end user incidents and requests are handled by the TfL IM Service Desk and for the TfL IM Service Desk to be the single point of contact for the bidder for these purposes.

The TFL IM Service Desk is responsible for:
• Single point of contact for management of and documented information relating to incidents and problems
• Escalations
• Simple "how to" type requests based on scripted knowledge base
• Dissemination of major incident information via IVR
The Bidder will need to confirm that they will work with TfL IM to prepare helpdesk scripts to
The bidder is required to align with the TfL Change Management process. See "Change Management Policy.pdf" contained within the attached zip file "Service Management Ref
The bidder is required to align with the TfL IM Release Management standard. *(Please note, the word document attachment is a supporting document to the main PDF document). See "Release Management 3rd Party.pdf" and "IM Release Management Standard.doc"
The bidder is required to align with the Major Incident Management process which is aligned to ITIL. See " TfL Major Incident Management Process.pdf" contained within the
The bidder is required to align with the Problem Management process which is aligned to ITIL. See " TfL Problem Management.pdf" contained within the attached zip file "Service
The bidder is required to align with the service and Business Continuity Plans and Processes. See "ISO 27001 Section 9 Business Continuity Management Principles.pdf"
TfL requires a range of technical support material to be produced as part of service transition into live support and for that collateral to be maintained during the life of the
TfL requires an end-to-end assistance during the pilot and testing phases that the system is configured and tested as per requirements prior to acceptance of the product. This includes
The design must be compatible with TfL's standard monitoring systems, known as Ionix and SCOM 2012.
The system must adhere to the appropriate TfL IM security policies (e.g. Data Protection Act 1998 and Human Rights Act). See "Information Security Policy.pdf" and "Information Security Controls Framework.docx" contained within the attached zip file "Service
The system must ensure compliance with the TfL IM Security Classification of the data. See "TfL Standard – Information Security Classification.pdf" contained within the attached

	Method of Delivery		
Compliance Level (Fully/Partial/Non Compliant)	**Out of the box (Y/N)**	**Configuration Required (Y/N)**	**Custom Development (Y/N)**

Tender Responses

Integration Development (Y/N)	**Met Requirement Comments**

Un-met Requirement Comments

APPENDIX G

Draft Project Plan

ID	Task Mode	Task Name	Duration
1		Access Planning Solution Delivery	264 days
2		Embed RMCon Resources	24 days
3		Consolidated Plan	46 days
10		Design Phase	216 days
21		Data Migration	65 days
39		Sprints (Including Customisations)	54 days
52		Test	90 days
87		Environments	79 days
125		Comms	1 day?
127		<New Task>	
128		Cutover	46 days
178		Final Cutover	33.5 days
179		System and network Administration	11 days
180		Verify Printing/Faxing is working	2 days
181		Verify user Printing/Faxing defaults are set up	2 days
182		Ensure all network communications are in place	3 days
183		Ensure external access to system available	4 days
184		Ensure remote printers/services are available	0 days
185		TfL Application Branding (TfL Logo on Application)	5 days
186		Convert and Verify Data	2 days
187		Verify legacy pre-conversion data cleanup has been completed	0 days
188		Describe the data conversion sequence	0 days
189		Sequence download programs	0 days
190		Sequence of interface table creation programs	0 days
191		Sequence upload programs	0 days
192		Sequence translation programs	0 days

Project: IM MS PLan Access P
Date: Thu 17/12/15

Task		External Milestone		Manual Summary Rollup	
Split		Inactive Task		Manual Summary	
Milestone		Inactive Milestone		Start-only	
Summary		Inactive Summary		Finish-only	
Project Summary		Manual Task		Deadline	
External Tasks		Duration-only		Progress	

ID	Task Mode	Task Name	Duration
193		Sequence interface/validation programs	0 days
194		Run the conversions (see Data Migration Plan)	1 day
195		Enter manual conversions (see Data Migration Plan)	1 day
196		Verify the converted data (see Data Migration Plan)	1 day
197		Secure acceptance that the converted and verified data meets compliance standards.	0 days
198		**Verify Production Readiness**	**1.5 days**
199		Review the production readiness verification checklist	0.5 days
200		Conduct production readiness verification	0.5 days
201		Confirm the production cutover	0.5 days
202		Prepare the support team	1 day
203		Obtain agreement for the initial production schedule	0 days
204		Verify that users are trained	0 days
205		Verify commitment and readiness of internal and external support personnel	0.5 days
206		Verify the completion of the production environment	0.5 days
207		Confirm senior management commitment via the steering committee	0 days
208		Distribute the initial production schedule	0 days
209		Obtain approval for beginning production	0 days
210		**Switch On**	**21 days**
211		Initiate using the production system	0.5 days
212		Initiate incident/technical issue management procedures	0 days
213		Initiate open issues and create a resolution list	0 days
214		Initiate support model (1st line, 2nd line etc.)	0 days
215		Confirm that all components of the production system are operational - Sanity Check	0.5 days
216		Communicate the new system live	0 days
217		Parallel Running if Required	20 days
218		**Training (AP Application Only - Standalone?)**	**62 days**

Project: IM MS PLan Access P
Date: Thu 17/12/15

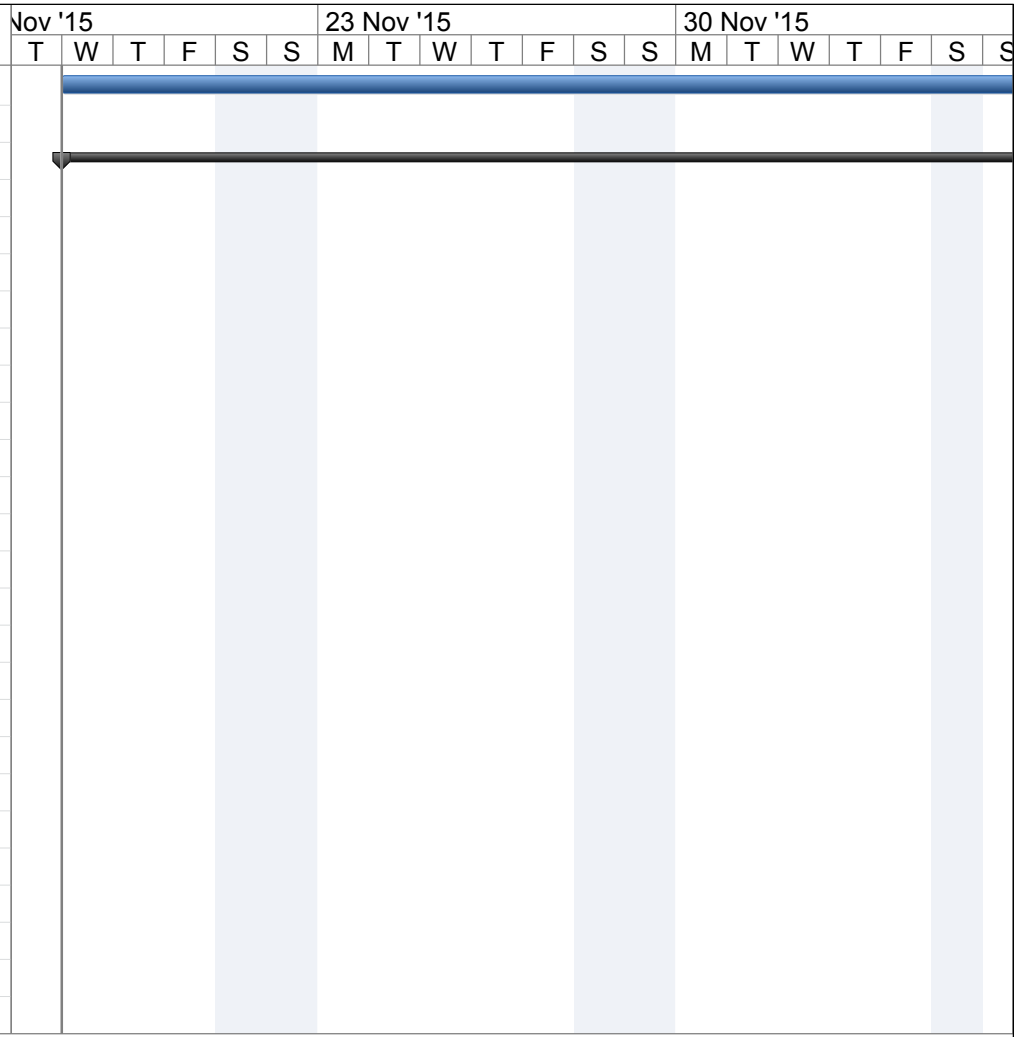
Task		External Milestone		Manual Summary Rollup	
Split		Inactive Task		Manual Summary	
Milestone		Inactive Milestone		Start-only	
Summary		Inactive Summary		Finish-only	
Project Summary		Manual Task		Deadline	
External Tasks		Duration-only		Progress	

ID	Task Mode	Task Name	Duration
229		Warranty	46.5 days?
240		Checkpoints	201.5 days
247		Post Go-Live	16 days

Project: IM MS PLan Access P
Date: Thu 17/12/15

Task		External Milestone		Manual Summary Rollup	
Split		Inactive Task		Manual Summary	
Milestone		Inactive Milestone		Start-only	
Summary		Inactive Summary		Finish-only	
Project Summary		Manual Task		Deadline	
External Tasks		Duration-only		Progress	

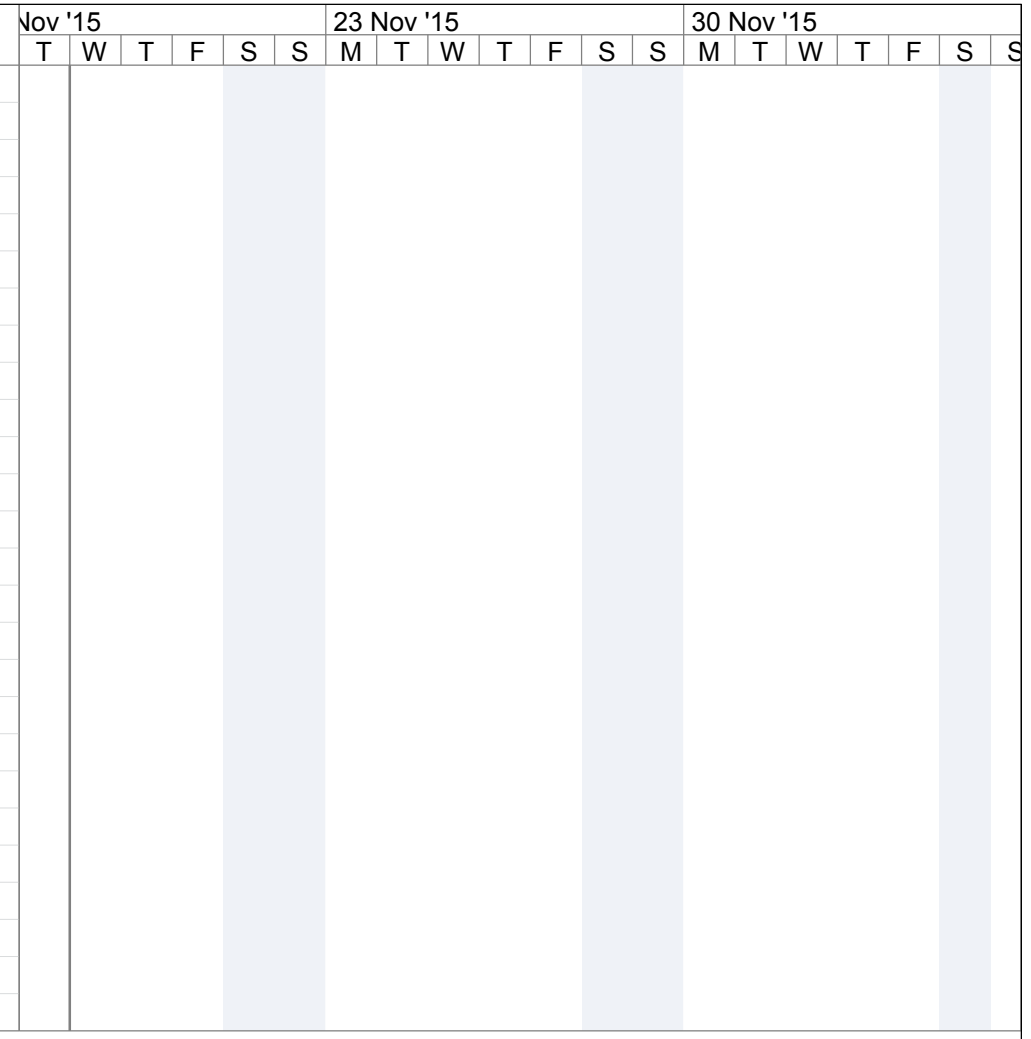
Start	Finish	Predecessors	Resource Names
Wed 18/11/15	Tue 22/11/16		
Mon 07/12/15	Fri 08/01/16		IM, AP, RMCon
Wed 18/11/15	Thu 21/01/16		
Mon 04/01/16	Mon 31/10/16		
Tue 01/03/16	Mon 30/05/16		
Fri 05/02/16	Wed 20/04/16		
Thu 28/04/16	Thu 01/09/16		
Tue 17/05/16	Fri 02/09/16		
Fri 18/12/15	Fri 18/12/15		
Fri 29/07/16	Fri 30/09/16		
Wed 14/09/16	Mon 31/10/16		
Wed 14/09/16	Wed 28/09/16		
Wed 14/09/16	Thu 15/09/16	143	AP, RMCon,IM
Wed 14/09/16	Thu 15/09/16	143	AP, RMCon,IM
Thu 22/09/16	Mon 26/09/16	151	AP, RMCon,IM
Thu 22/09/16	Tue 27/09/16	151	AP, RMCon,IM
Thu 15/09/16	Thu 15/09/16	180	AP, RMCon,IM
Thu 22/09/16	Wed 28/09/16	151	RMCon
Tue 27/09/16	Thu 29/09/16		
Tue 27/09/16	Tue 27/09/16	160	RMCon
Tue 27/09/16	Tue 27/09/16	160	RMCon
Tue 27/09/16	Tue 27/09/16	160	RMCon
Tue 27/09/16	Tue 27/09/16	160	RMCon
Tue 27/09/16	Tue 27/09/16	160	RMCon
Tue 27/09/16	Tue 27/09/16	160	RMCon



Project: IM MS PLan Access P
Date: Thu 17/12/15

Task	External Milestone	Manual Summary Rollup	
Split	Inactive Task	Manual Summary	
Milestone	Inactive Milestone	Start-only	
Summary	Inactive Summary	Finish-only	
Project Summary	Manual Task	Deadline	
External Tasks	Duration-only	Progress	

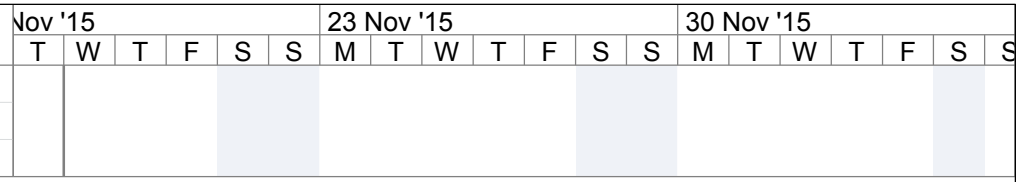
Start	Finish	Predecessors	Resource Names
Tue 27/09/16	Tue 27/09/16	160	RMCon
Wed 28/09/16	Wed 28/09/16	193	RMCon
Wed 28/09/16	Wed 28/09/16	193	RMCon
Thu 29/09/16	Thu 29/09/16	194,195	RMCon
Thu 29/09/16	Thu 29/09/16	196	RMCon
Thu 29/09/16	**Mon 03/10/16**		
Fri 30/09/16	Fri 30/09/16	197	AP, RMCon,IM
Fri 30/09/16	Fri 30/09/16	197	AP, RMCon,GIS,IM
Fri 30/09/16	Fri 30/09/16	197	AP, RMCon,GIS,IM
Fri 30/09/16	Fri 30/09/16	197	RMCon,IM
Thu 29/09/16	Thu 29/09/16	197	RMCon,IM
Thu 29/09/16	Thu 29/09/16	197	RMCon,IM, AP
Mon 03/10/16	Mon 03/10/16	202	RMCon,IM
Fri 30/09/16	Fri 30/09/16	203	RMCon
Fri 30/09/16	Fri 30/09/16	206	IM
Fri 30/09/16	Fri 30/09/16	206	RMCon,IM
Fri 30/09/16	Fri 30/09/16	207	IM
Fri 30/09/16	**Mon 31/10/16**		
Fri 30/09/16	Fri 30/09/16	209	AP, RMCon,GIS,IM
Fri 30/09/16	Fri 30/09/16	211	AP, RMCon,GIS,IM
Fri 30/09/16	Fri 30/09/16	211	RMCon,IM
Fri 30/09/16	Fri 30/09/16	211	AP, RMCon,IM
Mon 03/10/16	Mon 03/10/16	211	AP, RMCon,GIS,IM
Mon 03/10/16	Mon 03/10/16	215	IM
Mon 03/10/16	Mon 31/10/16	216	AP,IM
Mon 04/04/16	**Tue 28/06/16**		



Project: IM MS PLan Access P
Date: Thu 17/12/15

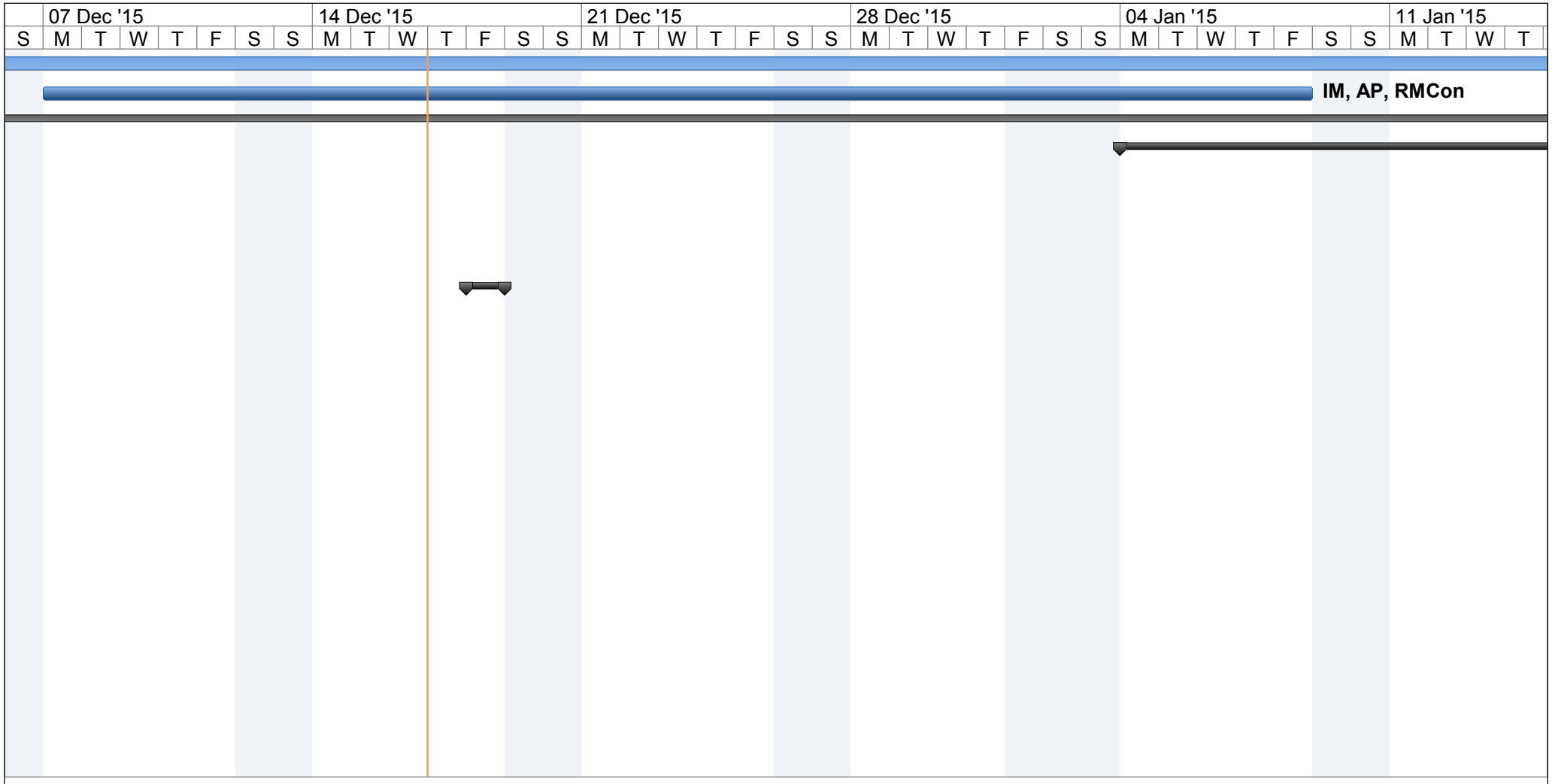
Task	External Milestone	Manual Summary Rollup	
Split	Inactive Task	Manual Summary	
Milestone	Inactive Milestone	Start-only	
Summary	Inactive Summary	Finish-only	
Project Summary	Manual Task	Deadline	
External Tasks	Duration-only	Progress	

Start	Finish	Predecessors	Resource Names
Thu 25/08/16	Mon 31/10/16		
Thu 21/01/16	Mon 31/10/16		
Mon 31/10/16	Tue 22/11/16		



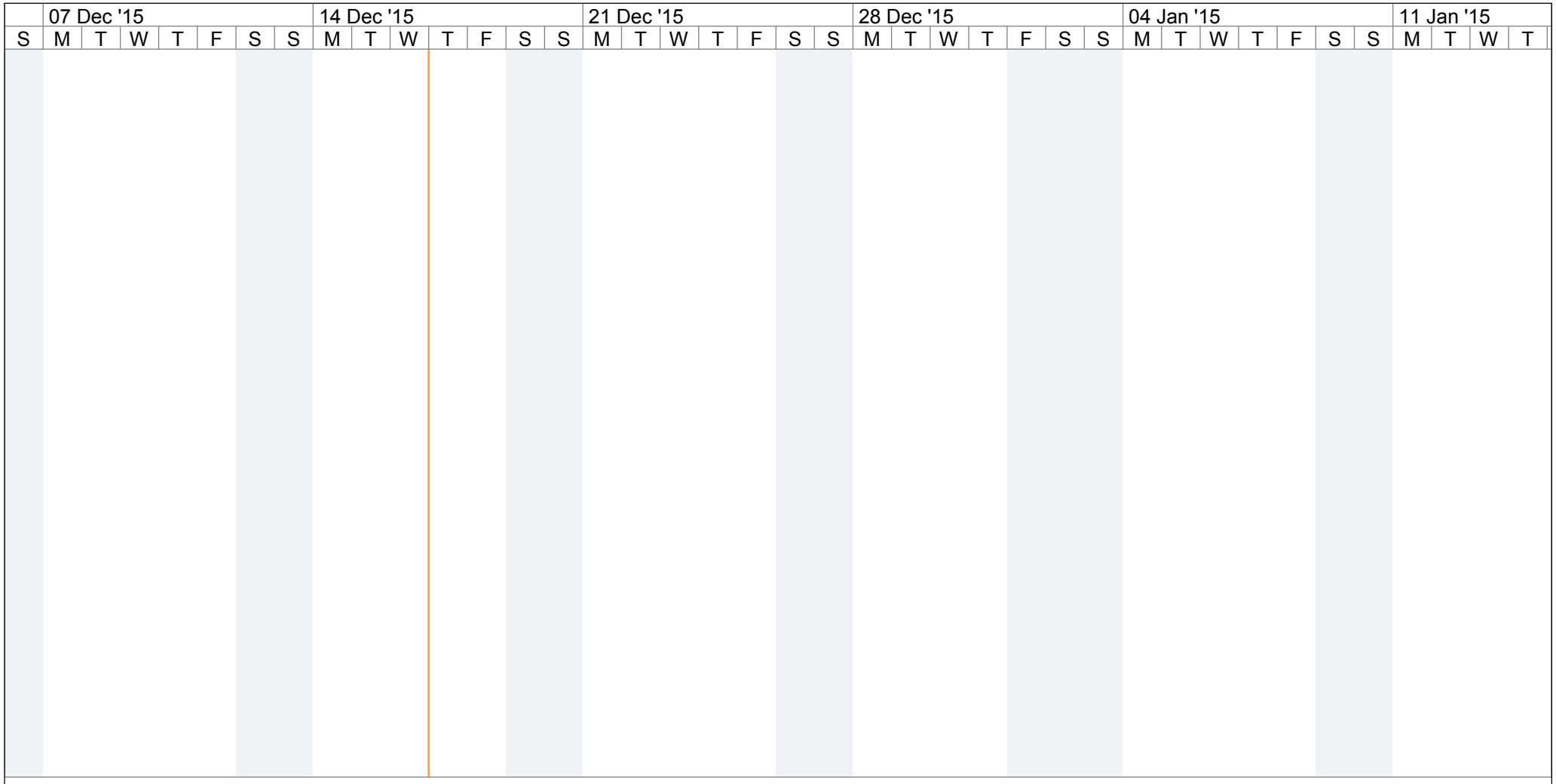
Project: IM MS PLan Access P
Date: Thu 17/12/15

Task		External Milestone		Manual Summary Rollup	
Split		Inactive Task		Manual Summary	
Milestone		Inactive Milestone		Start-only	
Summary		Inactive Summary		Finish-only	
Project Summary		Manual Task		Deadline	
External Tasks		Duration-only		Progress	



Project: IM MS PLan Access P
Date: Thu 17/12/15

Task		External Milestone		Manual Summary Rollup	
Split		Inactive Task		Manual Summary	
Milestone		Inactive Milestone		Start-only	
Summary		Inactive Summary		Finish-only	
Project Summary		Manual Task		Deadline	
External Tasks		Duration-only		Progress	

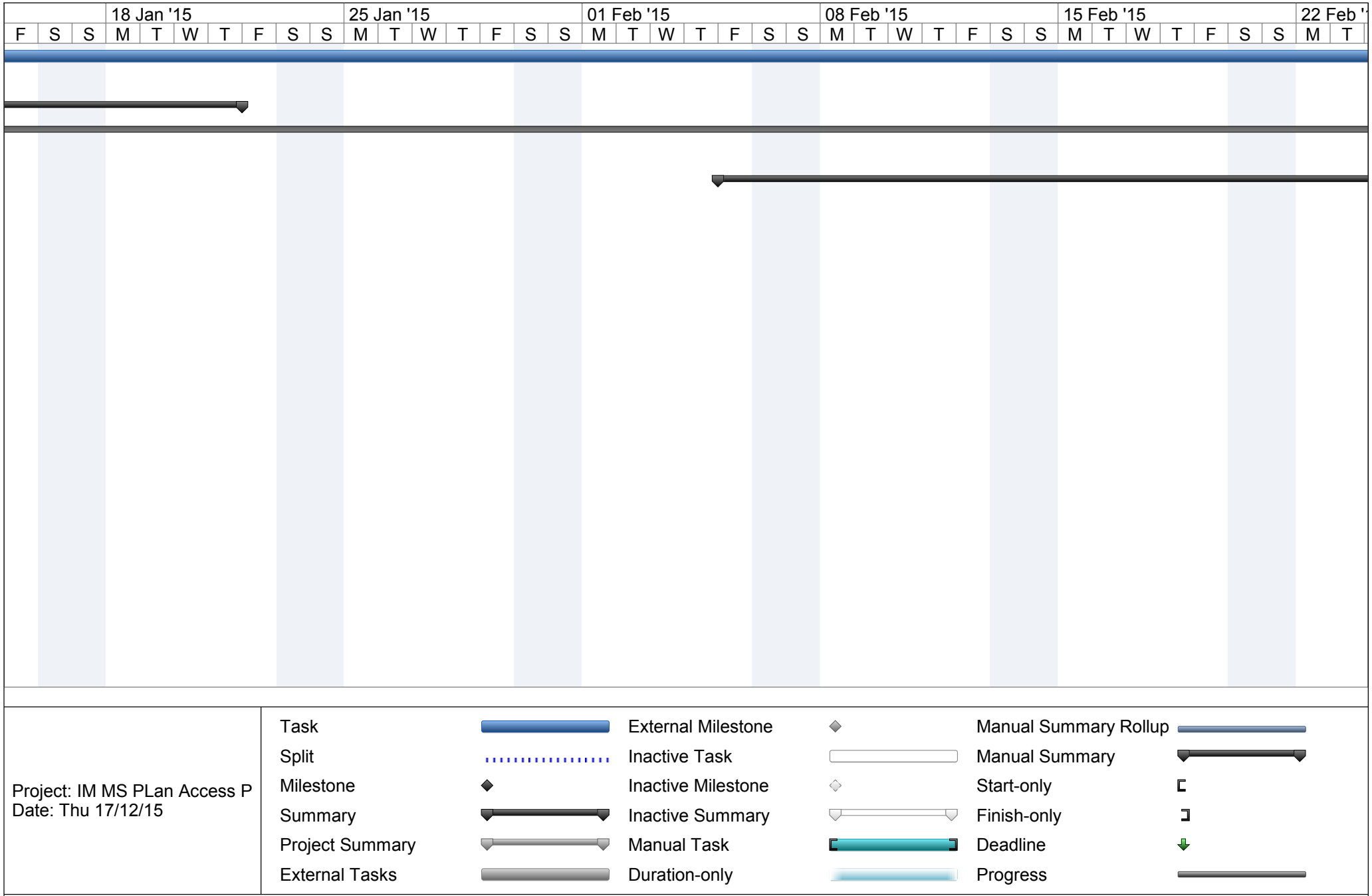


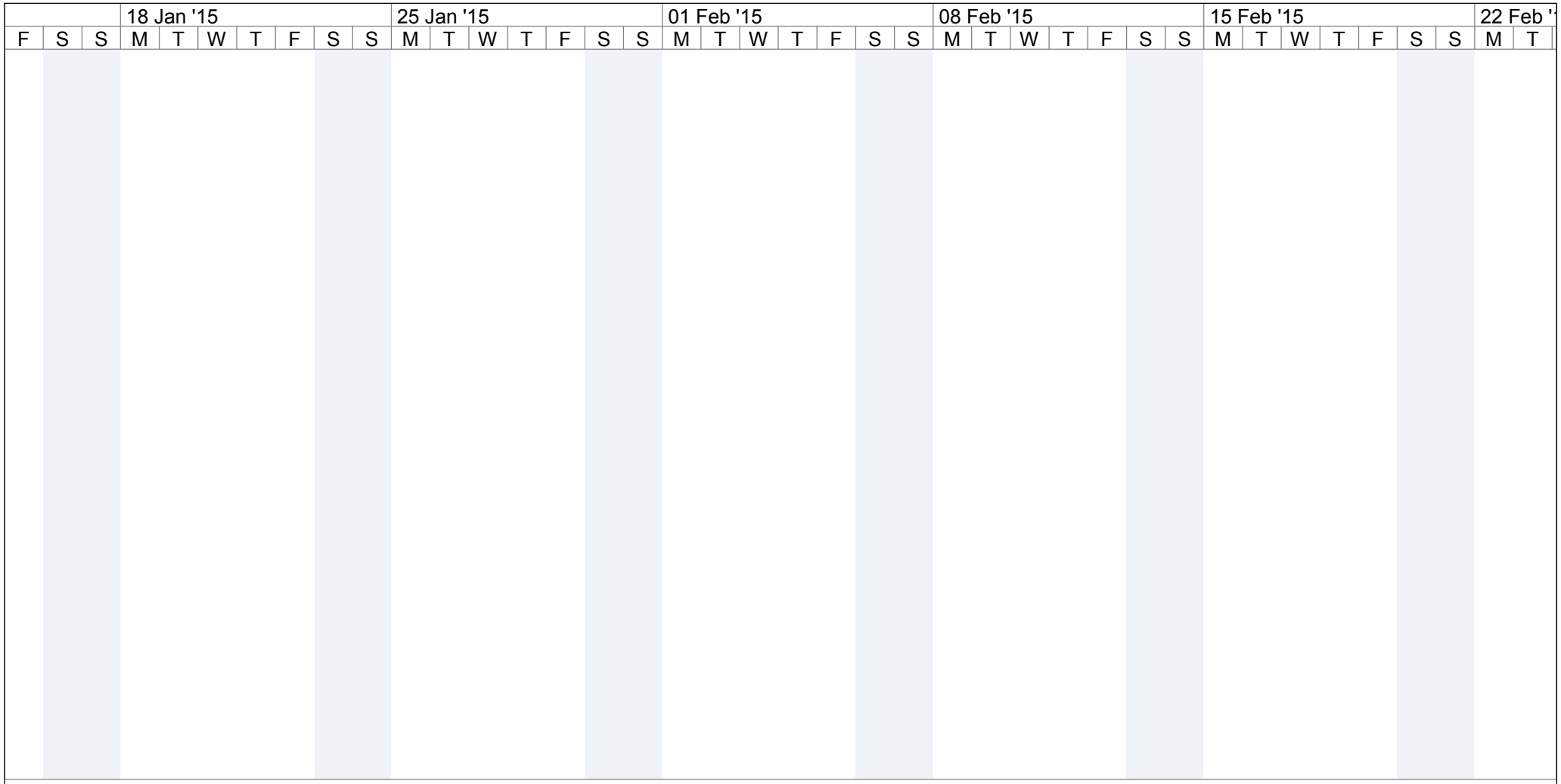
Project: IM MS PLan Access P
Date: Thu 17/12/15

Task	External Milestone	Manual Summary Rollup
Split	Inactive Task	Manual Summary
Milestone	Inactive Milestone	Start-only
Summary	Inactive Summary	Finish-only
Project Summary	Manual Task	Deadline
External Tasks	Duration-only	Progress

Project: IM MS PLan Access P
Date: Thu 17/12/15

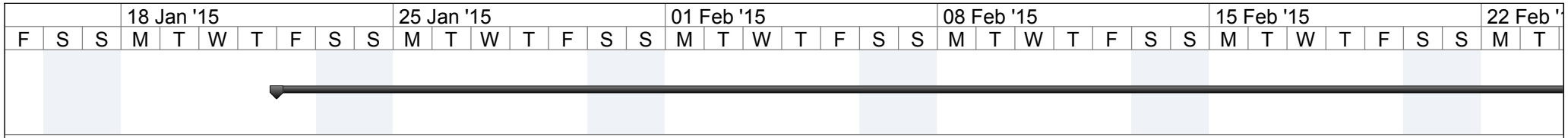
Task	External Milestone	Manual Summary Rollup
Split	Inactive Task	Manual Summary
Milestone	Inactive Milestone	Start-only
Summary	Inactive Summary	Finish-only
Project Summary	Manual Task	Deadline
External Tasks	Duration-only	Progress


18 Jan '15
25 Jan '15
01 Feb '15
08 Feb '15
15 Feb '15
22 Feb '
F S S M T W T F S S M T W T F S S M T W T F S S M T W T F S S M T W T F S S M T
Project: IM MS PLan Access P
Date: Thu 17/12/15
Task
Split
Milestone
Summary
Project Summary
External Tasks
External Milestone
Inactive Task
Inactive Milestone
Inactive Summary
Manual Task
Duration-only
Manual Summary Rollup
Manual Summary
Start-only
Finish-only
Deadline
Progress



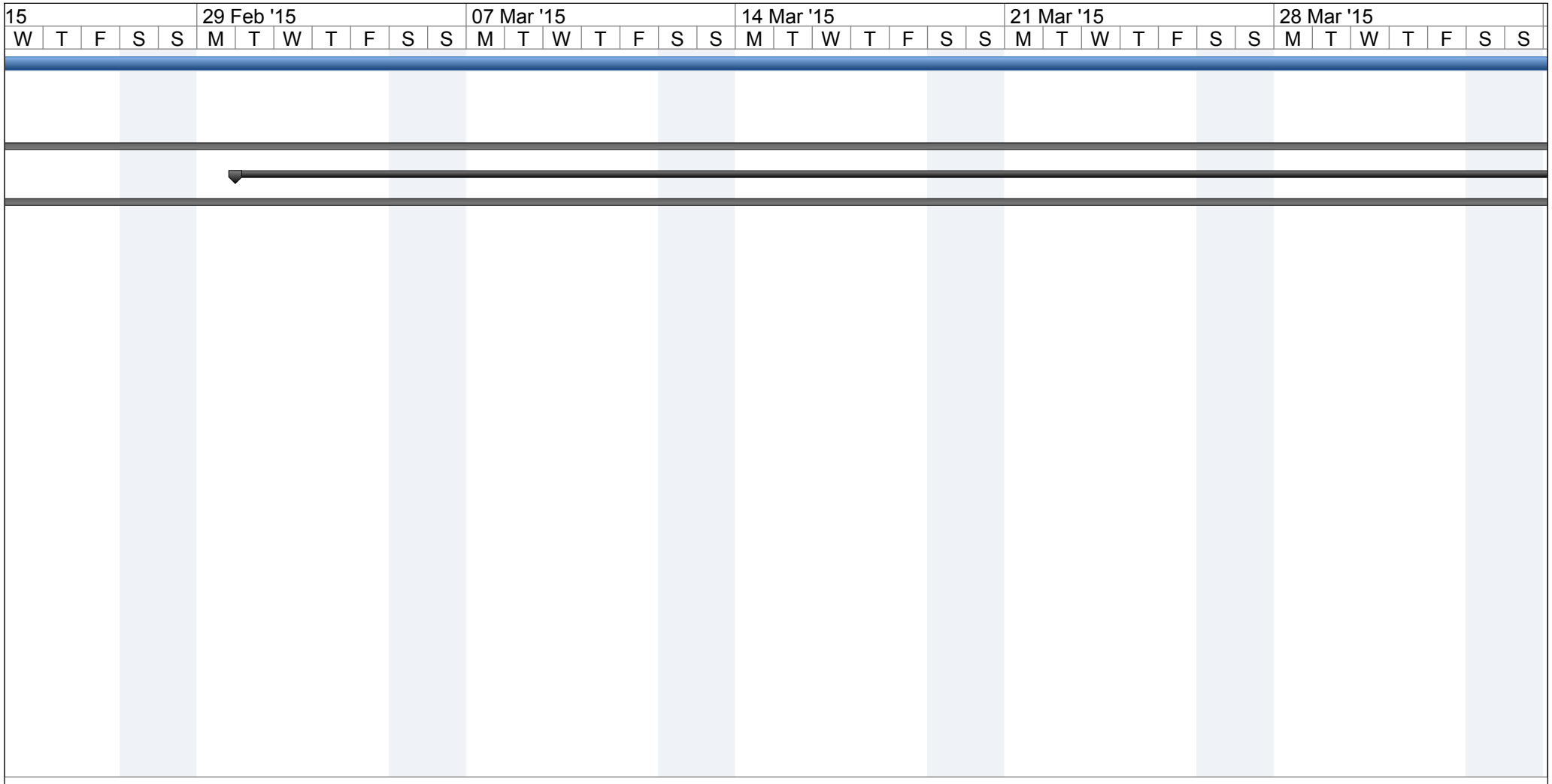
Project: IM MS PLan Access P
Date: Thu 17/12/15

Task		External Milestone		Manual Summary Rollup	
Split		Inactive Task		Manual Summary	
Milestone		Inactive Milestone		Start-only	
Summary		Inactive Summary		Finish-only	
Project Summary		Manual Task		Deadline	
External Tasks		Duration-only		Progress	



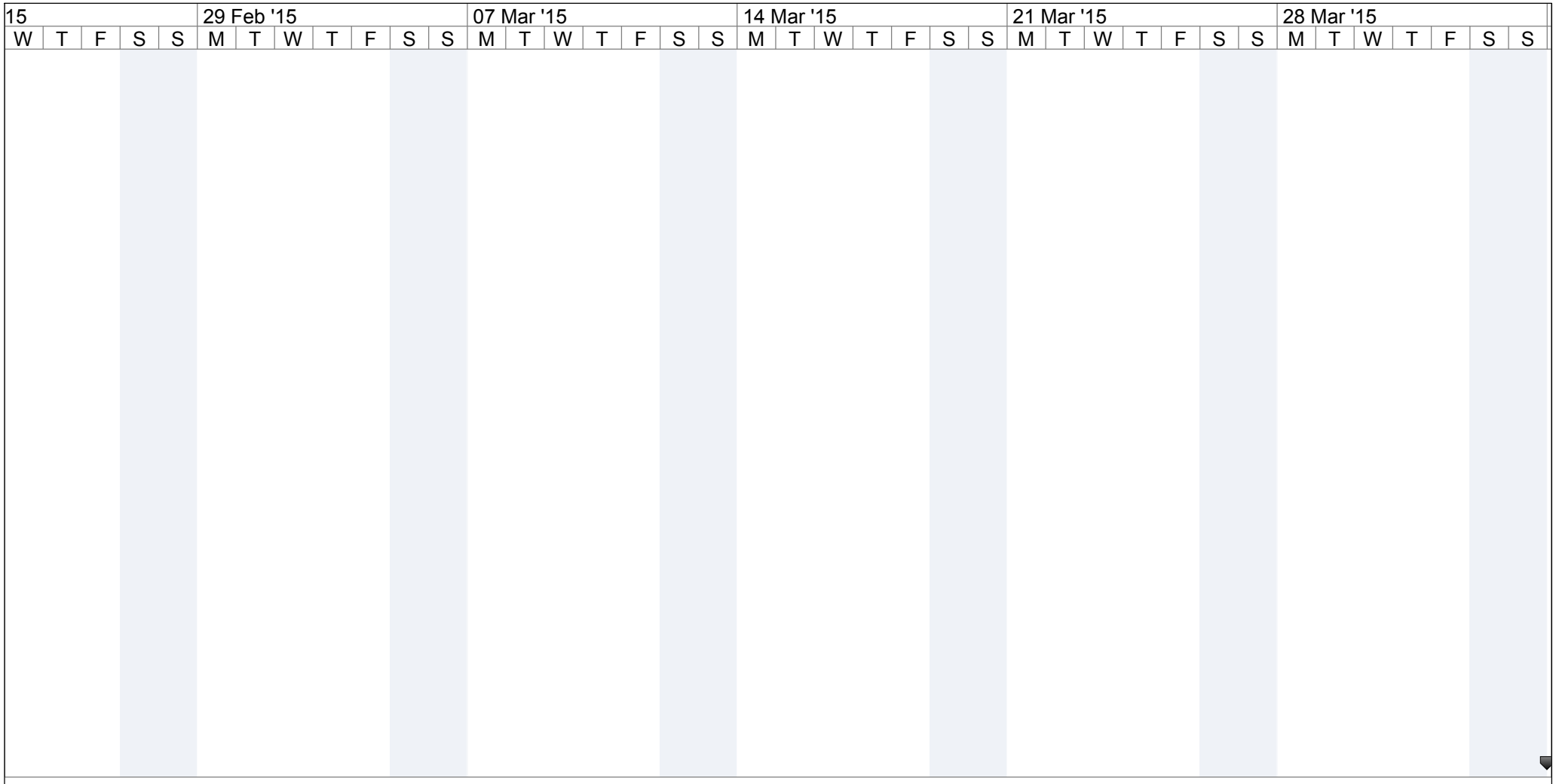
Project: IM MS PLan Access P
Date: Thu 17/12/15

Task	External Milestone	Manual Summary Rollup
Split	Inactive Task	Manual Summary
Milestone	Inactive Milestone	Start-only
Summary	Inactive Summary	Finish-only
Project Summary	Manual Task	Deadline
External Tasks	Duration-only	Progress



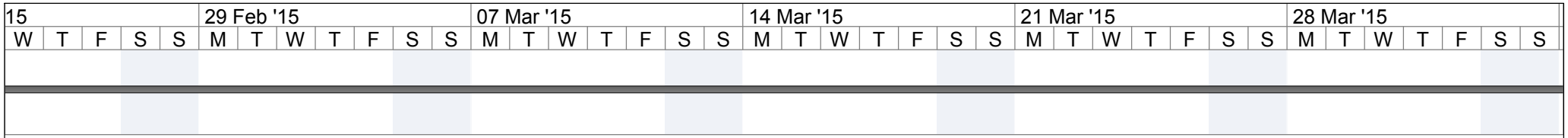
Project: IM MS PLan Access P
Date: Thu 17/12/15

Task		External Milestone		Manual Summary Rollup	
Split		Inactive Task		Manual Summary	
Milestone		Inactive Milestone		Start-only	
Summary		Inactive Summary		Finish-only	
Project Summary		Manual Task		Deadline	
External Tasks		Duration-only		Progress	



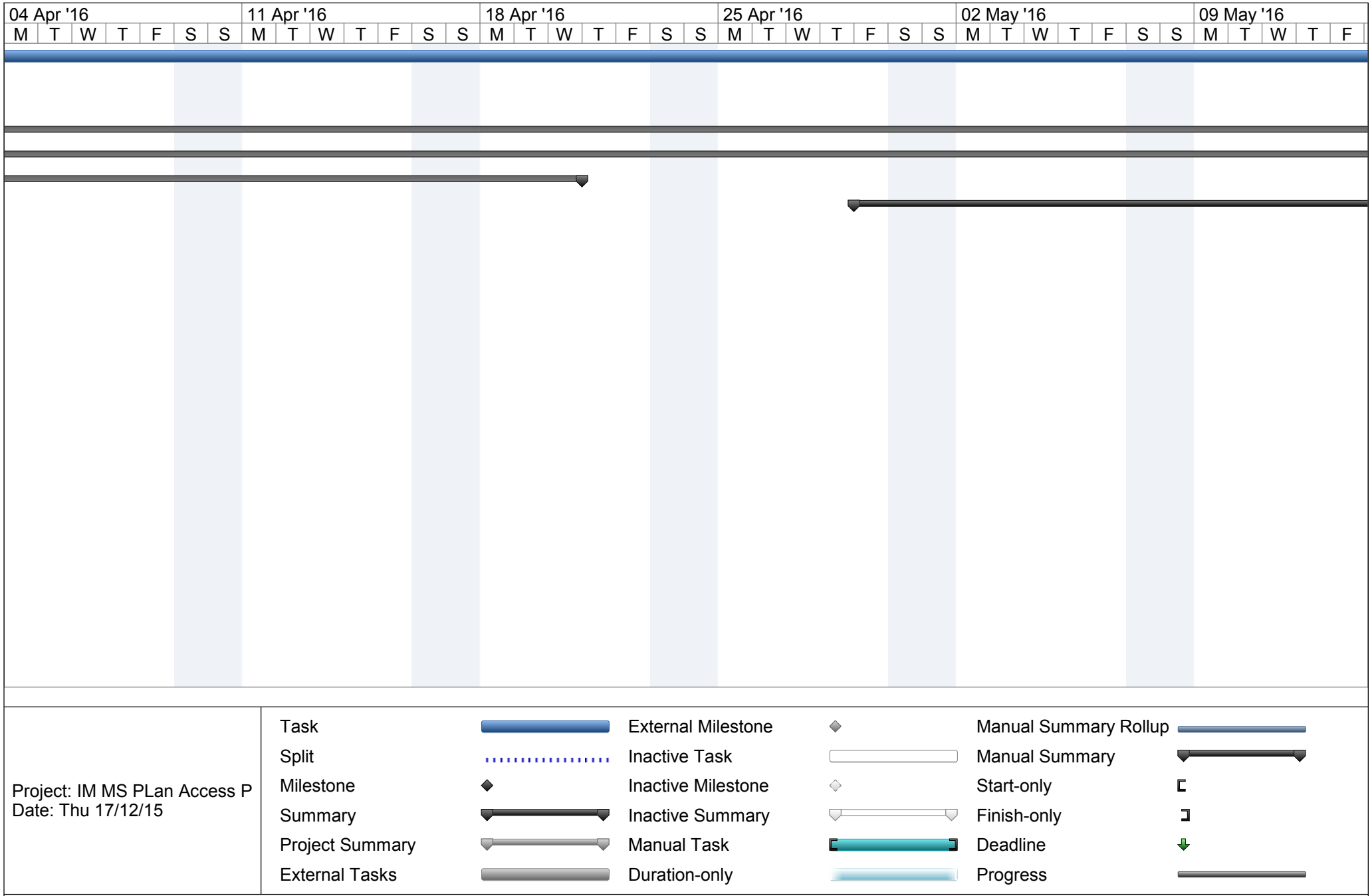
Project: IM MS PLan Access P
Date: Thu 17/12/15

Task		External Milestone		Manual Summary Rollup	
Split		Inactive Task		Manual Summary	
Milestone		Inactive Milestone		Start-only	
Summary		Inactive Summary		Finish-only	
Project Summary		Manual Task		Deadline	
External Tasks		Duration-only		Progress	



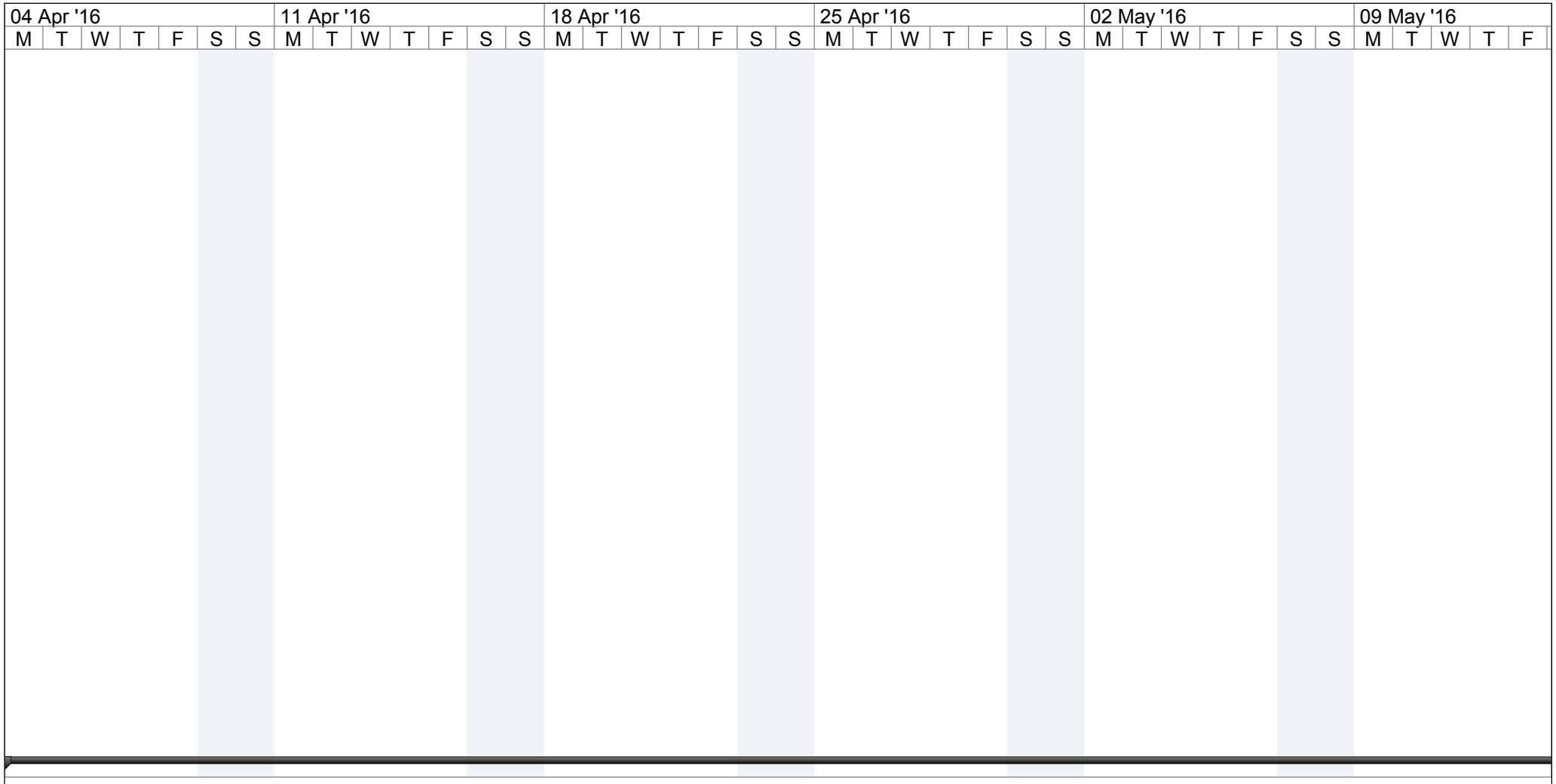
Project: IM MS PLan Access P
Date: Thu 17/12/15

Task		External Milestone		Manual Summary Rollup	
Split		Inactive Task		Manual Summary	
Milestone		Inactive Milestone		Start-only	
Summary		Inactive Summary		Finish-only	
Project Summary		Manual Task		Deadline	
External Tasks		Duration-only		Progress	



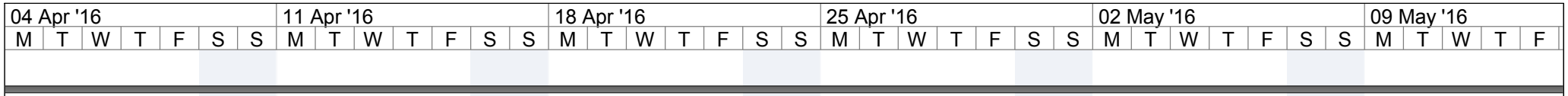
Project: IM MS PLan Access P
Date: Thu 17/12/15

Task		External Milestone		Manual Summary Rollup	
Split		Inactive Task		Manual Summary	
Milestone		Inactive Milestone		Start-only	
Summary		Inactive Summary		Finish-only	
Project Summary		Manual Task		Deadline	
External Tasks		Duration-only		Progress	



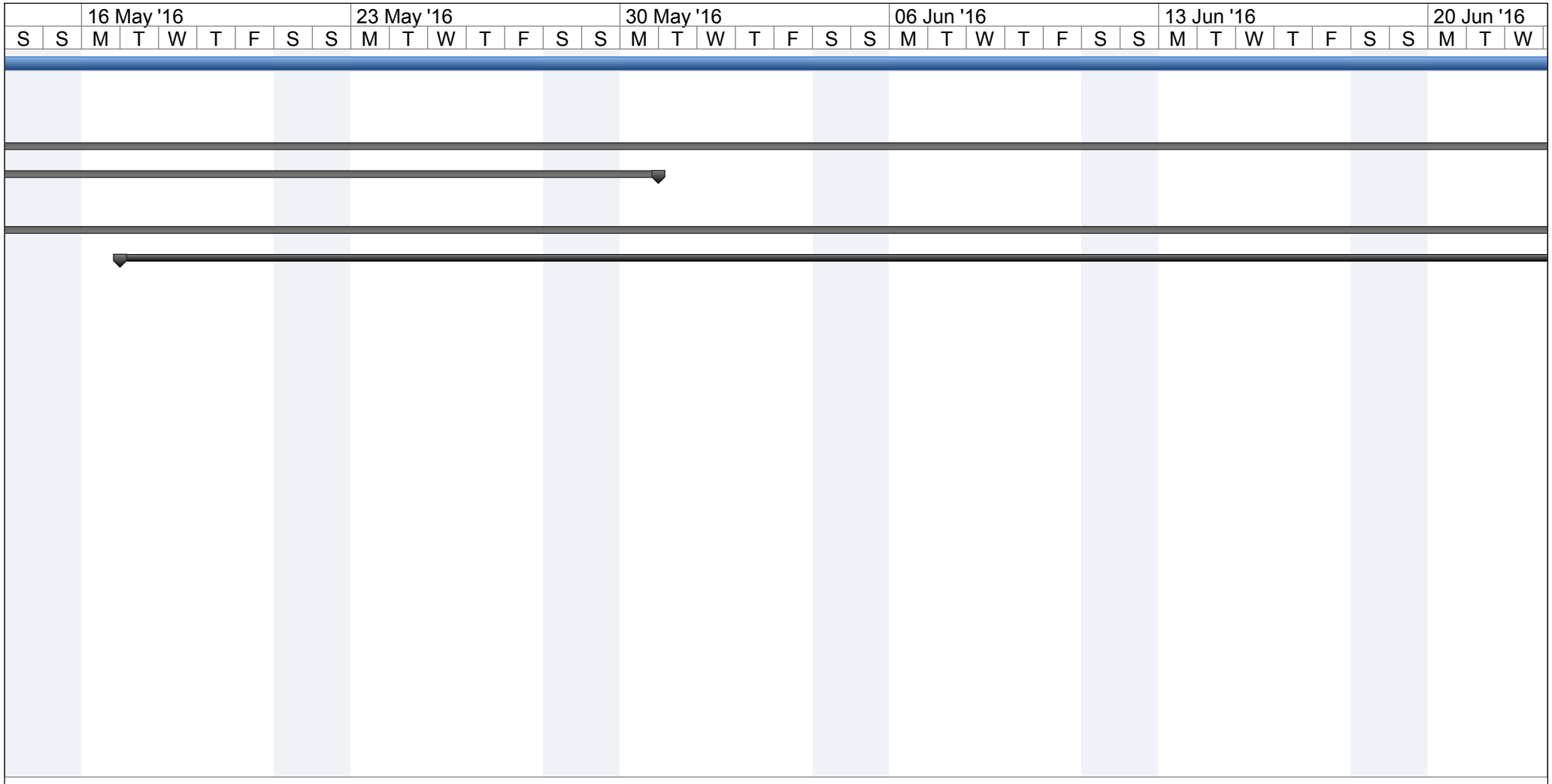
Project: IM MS PLan Access P
Date: Thu 17/12/15

Task	External Milestone	Manual Summary Rollup
Split	Inactive Task	Manual Summary
Milestone	Inactive Milestone	Start-only
Summary	Inactive Summary	Finish-only
Project Summary	Manual Task	Deadline
External Tasks	Duration-only	Progress



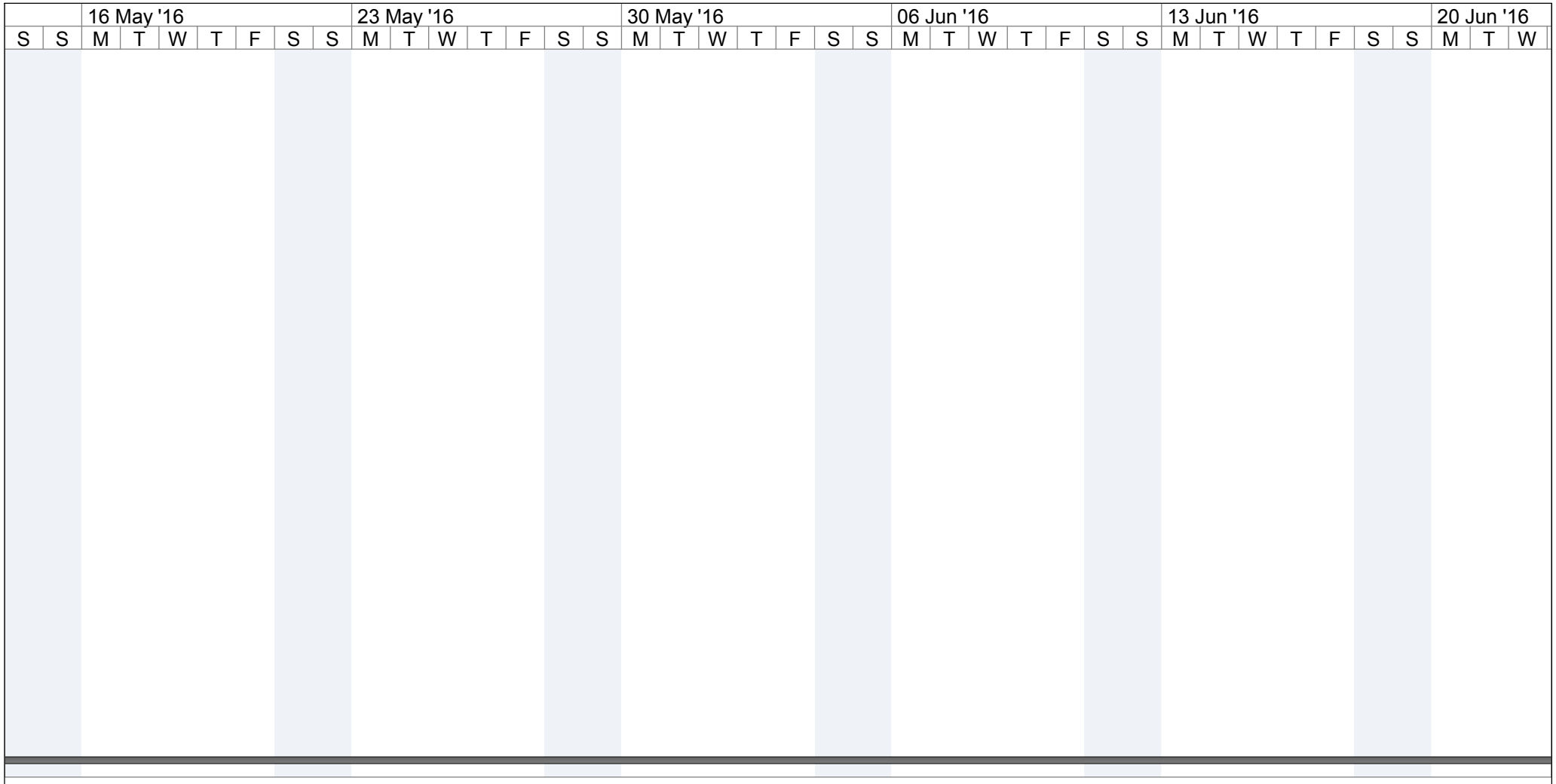
Project: IM MS PLan Access P
Date: Thu 17/12/15

Task		External Milestone		Manual Summary Rollup	
Split		Inactive Task		Manual Summary	
Milestone		Inactive Milestone		Start-only	
Summary		Inactive Summary		Finish-only	
Project Summary		Manual Task		Deadline	
External Tasks		Duration-only		Progress	



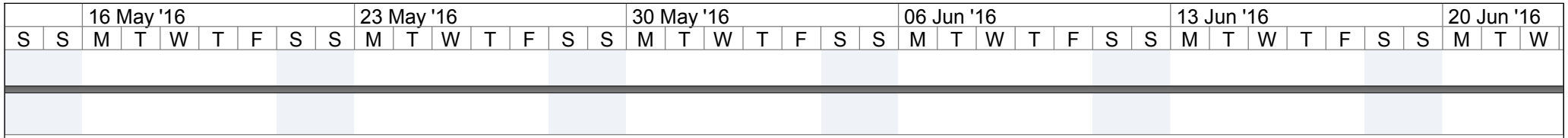
Project: IM MS PLan Access P
Date: Thu 17/12/15

Task		External Milestone		Manual Summary Rollup	
Split		Inactive Task		Manual Summary	
Milestone		Inactive Milestone		Start-only	
Summary		Inactive Summary		Finish-only	
Project Summary		Manual Task		Deadline	
External Tasks		Duration-only		Progress	



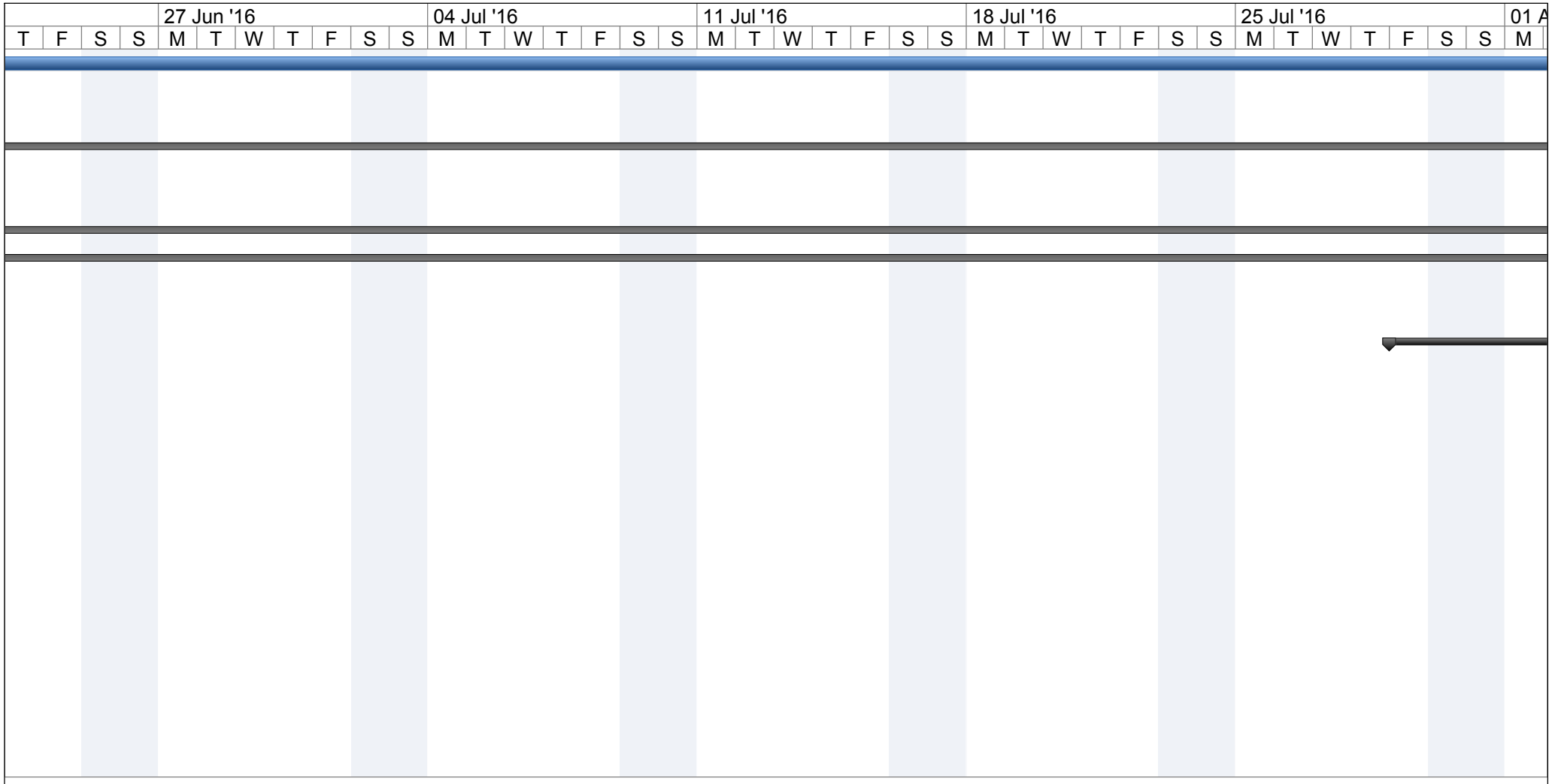
Project: IM MS PLan Access P
Date: Thu 17/12/15

Task		External Milestone		Manual Summary Rollup	
Split		Inactive Task		Manual Summary	
Milestone		Inactive Milestone		Start-only	
Summary		Inactive Summary		Finish-only	
Project Summary		Manual Task		Deadline	
External Tasks		Duration-only		Progress	



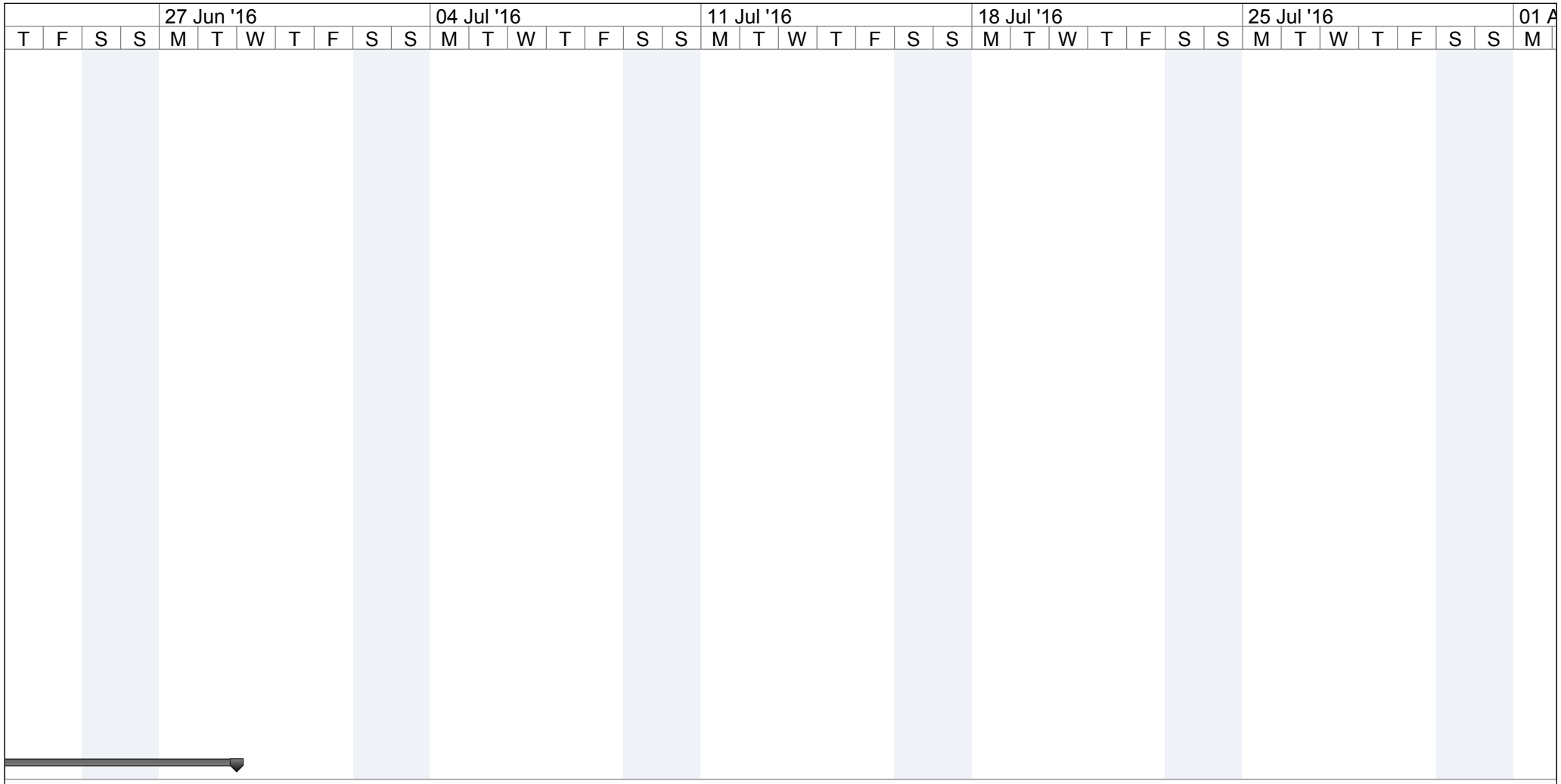
Project: IM MS PLan Access P
Date: Thu 17/12/15

Task		External Milestone		Manual Summary Rollup	
Split		Inactive Task		Manual Summary	
Milestone		Inactive Milestone		Start-only	
Summary		Inactive Summary		Finish-only	
Project Summary		Manual Task		Deadline	
External Tasks		Duration-only		Progress	



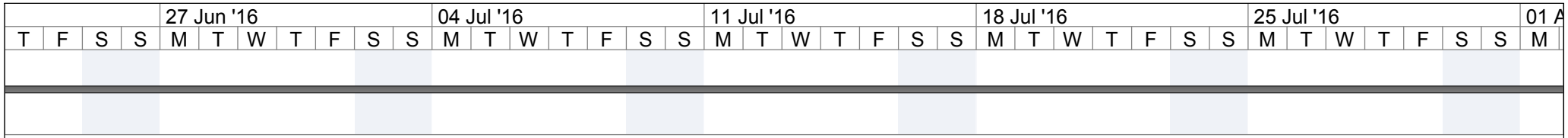
Project: IM MS PLan Access P
Date: Thu 17/12/15

Task		External Milestone		Manual Summary Rollup	
Split		Inactive Task		Manual Summary	
Milestone		Inactive Milestone		Start-only	
Summary		Inactive Summary		Finish-only	
Project Summary		Manual Task		Deadline	
External Tasks		Duration-only		Progress	



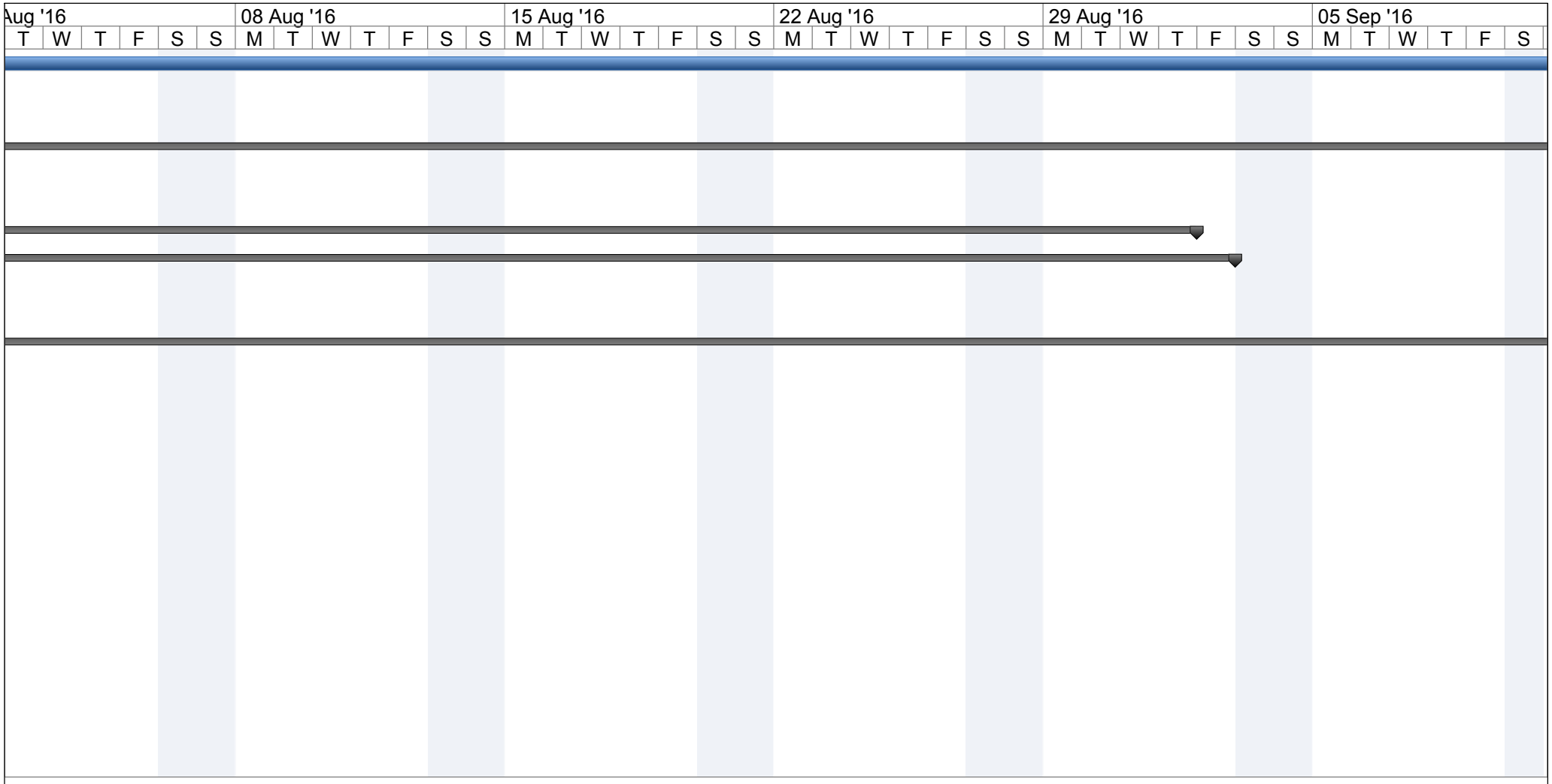
Project: IM MS PLan Access P
Date: Thu 17/12/15

Task		External Milestone		Manual Summary Rollup	
Split		Inactive Task		Manual Summary	
Milestone		Inactive Milestone		Start-only	
Summary		Inactive Summary		Finish-only	
Project Summary		Manual Task		Deadline	
External Tasks		Duration-only		Progress	



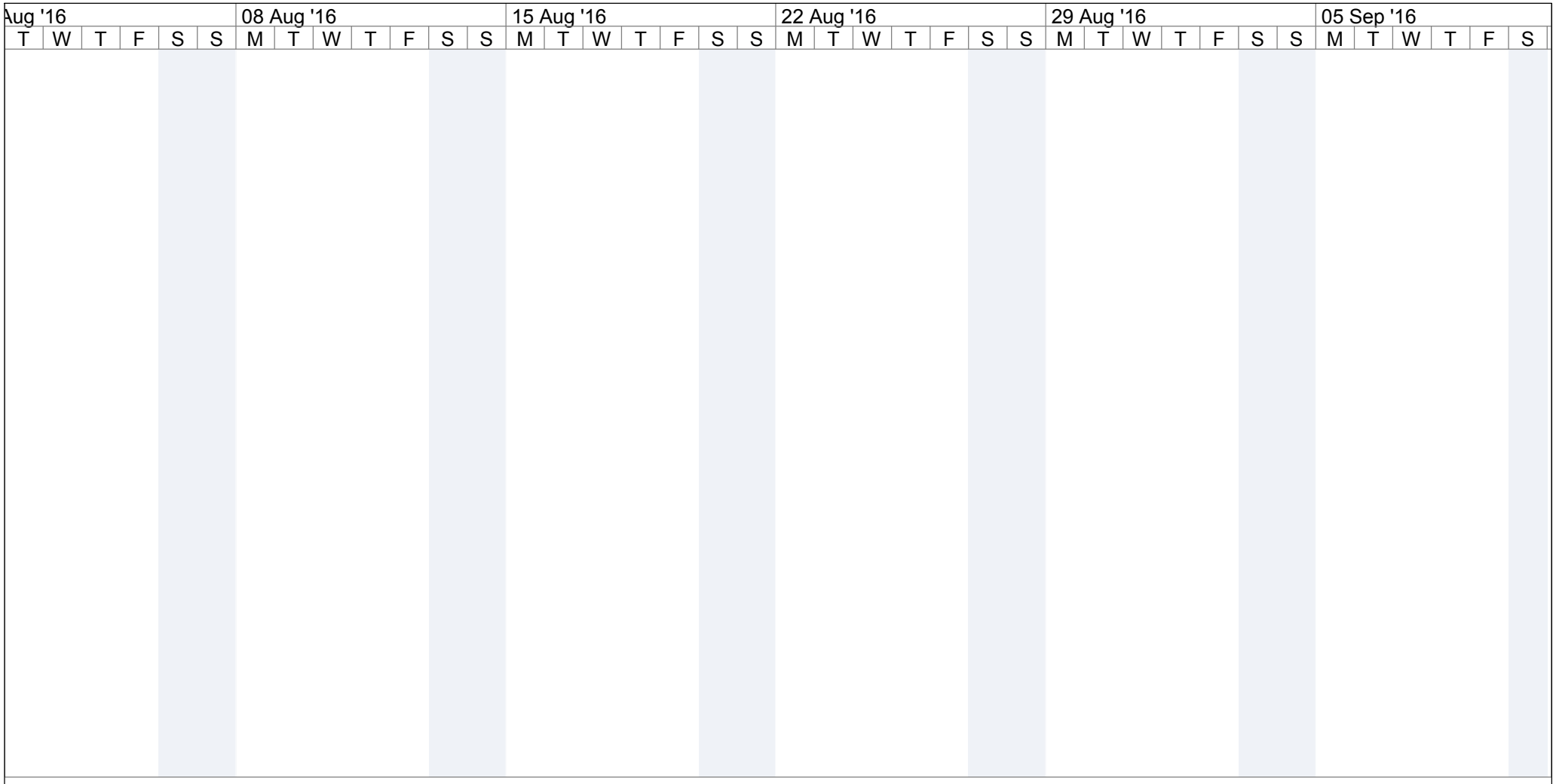
Project: IM MS PLan Access P
Date: Thu 17/12/15

Task		External Milestone		Manual Summary Rollup	
Split		Inactive Task		Manual Summary	
Milestone		Inactive Milestone		Start-only	
Summary		Inactive Summary		Finish-only	
Project Summary		Manual Task		Deadline	
External Tasks		Duration-only		Progress	



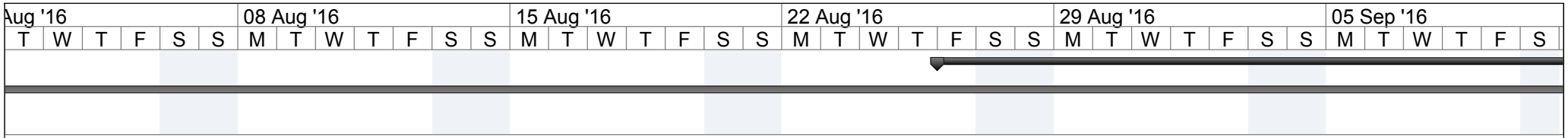
Project: IM MS PLan Access P
Date: Thu 17/12/15

Task		External Milestone		Manual Summary Rollup	
Split		Inactive Task		Manual Summary	
Milestone		Inactive Milestone		Start-only	
Summary		Inactive Summary		Finish-only	
Project Summary		Manual Task		Deadline	
External Tasks		Duration-only		Progress	



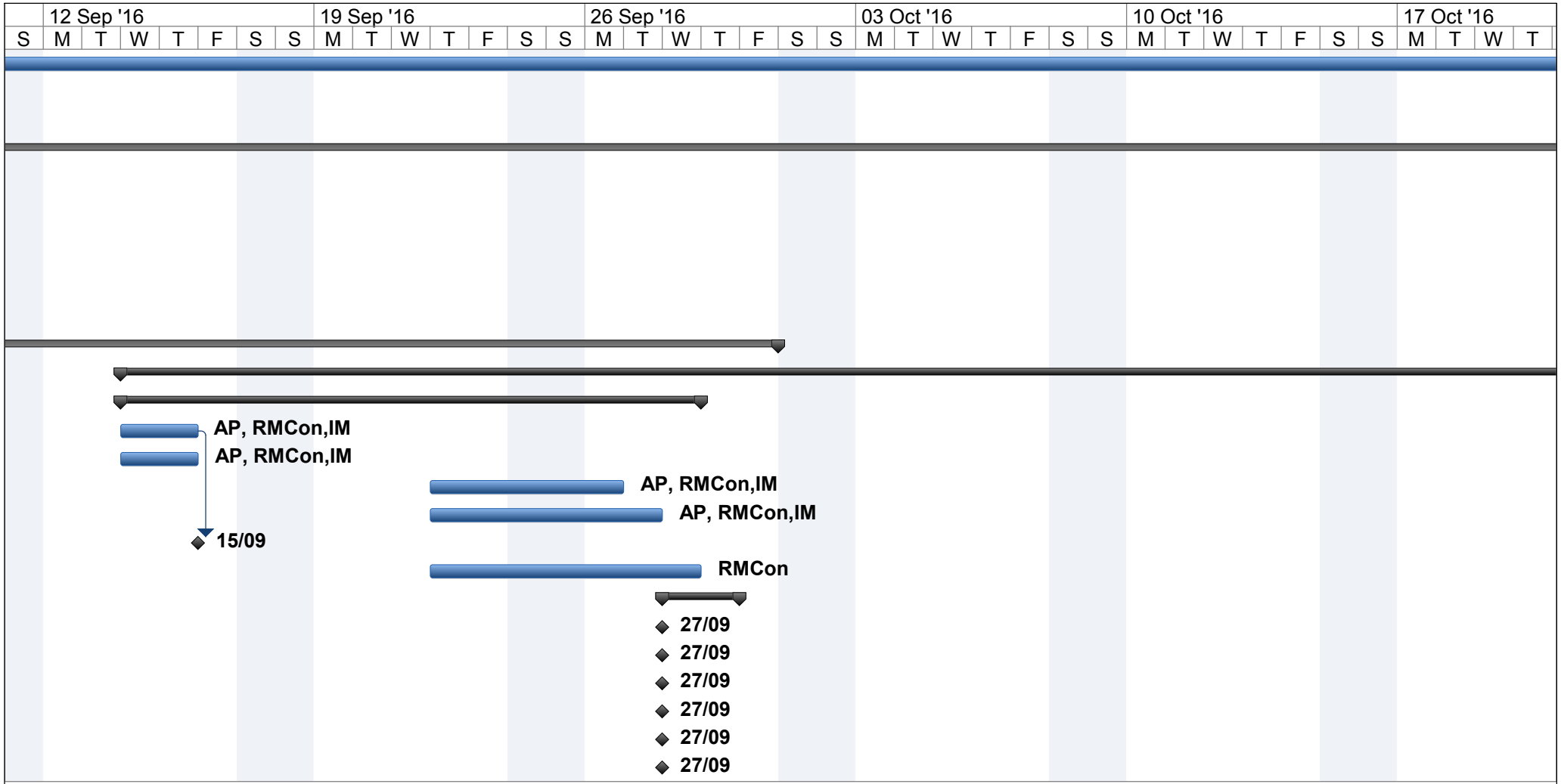
Project: IM MS PLan Access P
Date: Thu 17/12/15

Task		External Milestone		Manual Summary Rollup	
Split		Inactive Task		Manual Summary	
Milestone		Inactive Milestone		Start-only	
Summary		Inactive Summary		Finish-only	
Project Summary		Manual Task		Deadline	
External Tasks		Duration-only		Progress	



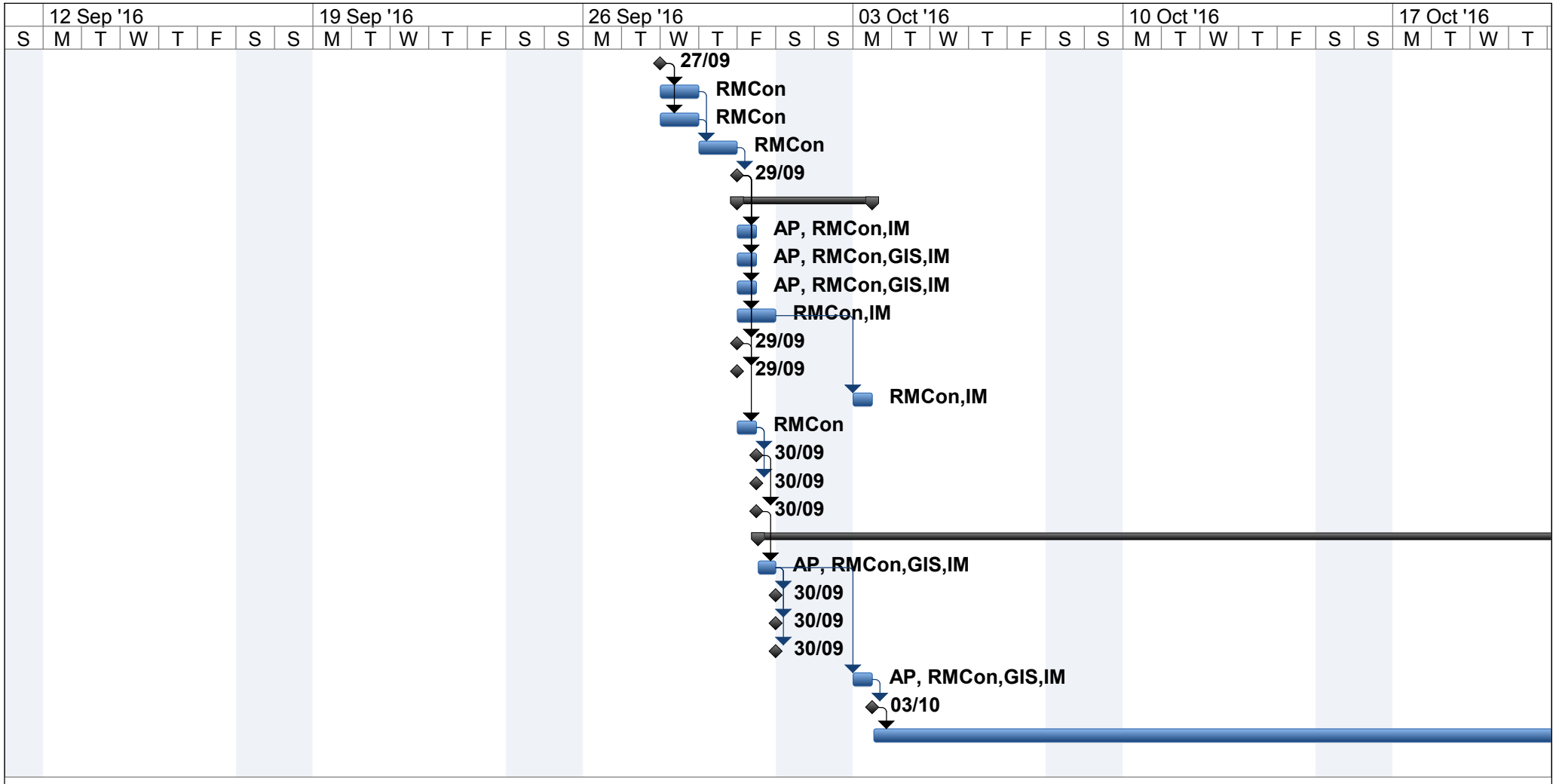
Project: IM MS PLan Access P
Date: Thu 17/12/15

Task		External Milestone		Manual Summary Rollup	
Split		Inactive Task		Manual Summary	
Milestone		Inactive Milestone		Start-only	
Summary		Inactive Summary		Finish-only	
Project Summary		Manual Task		Deadline	
External Tasks		Duration-only		Progress	



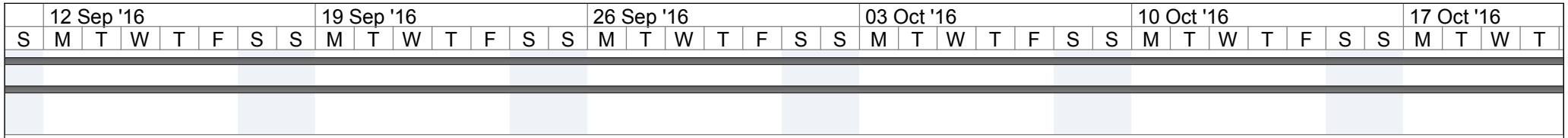
Project: IM MS PLan Access P
Date: Thu 17/12/15

Task	External Milestone	Manual Summary Rollup
Split	Inactive Task	Manual Summary
Milestone	Inactive Milestone	Start-only
Summary	Inactive Summary	Finish-only
Project Summary	Manual Task	Deadline
External Tasks	Duration-only	Progress



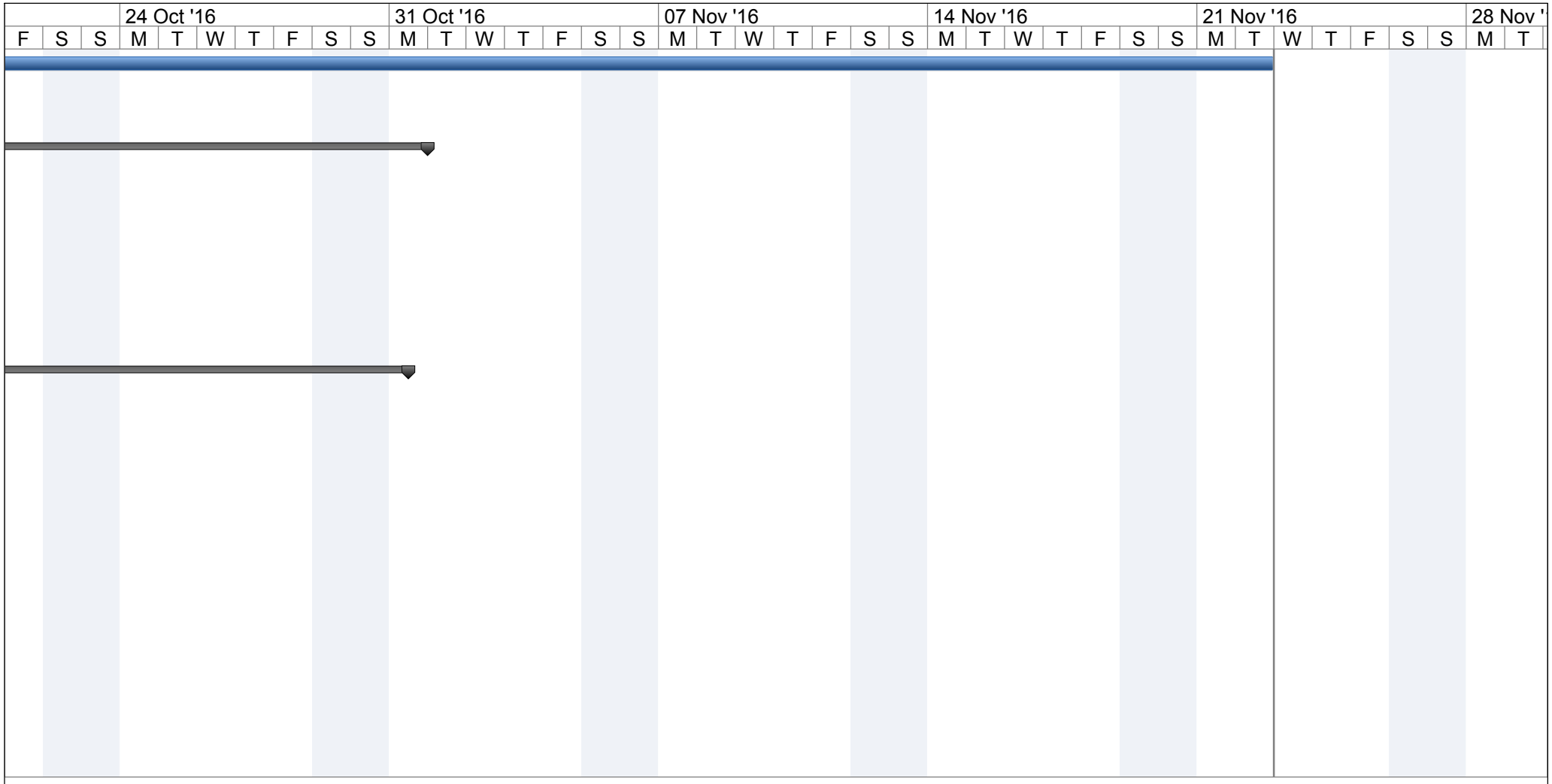
Project: IM MS PLan Access P
Date: Thu 17/12/15

Task	External Milestone	Manual Summary Rollup
Split	Inactive Task	Manual Summary
Milestone	Inactive Milestone	Start-only
Summary	Inactive Summary	Finish-only
Project Summary	Manual Task	Deadline
External Tasks	Duration-only	Progress



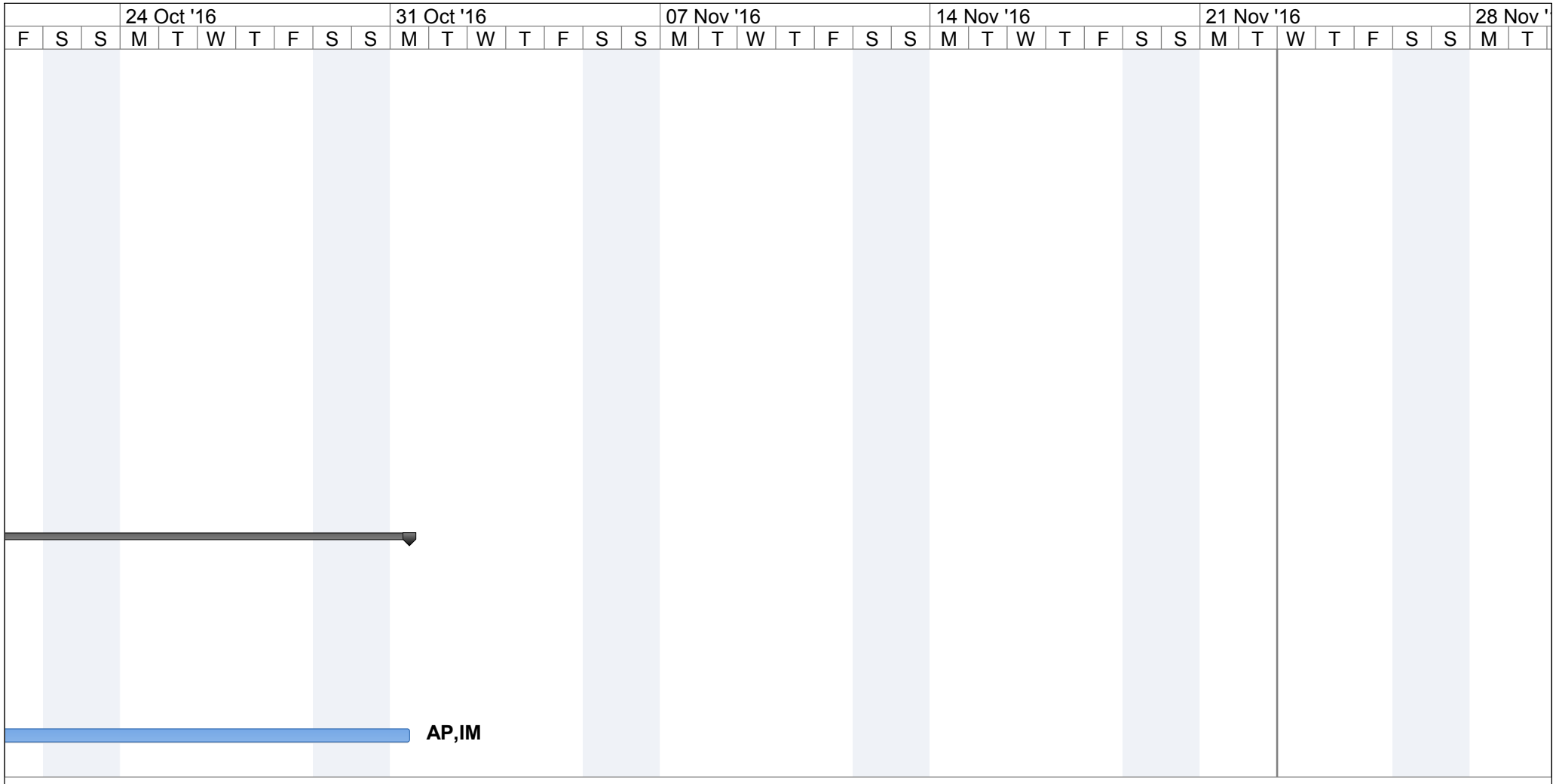
Project: IM MS PLan Access P
Date: Thu 17/12/15

Task		External Milestone		Manual Summary Rollup	
Split		Inactive Task		Manual Summary	
Milestone		Inactive Milestone		Start-only	
Summary		Inactive Summary		Finish-only	
Project Summary		Manual Task		Deadline	
External Tasks		Duration-only		Progress	



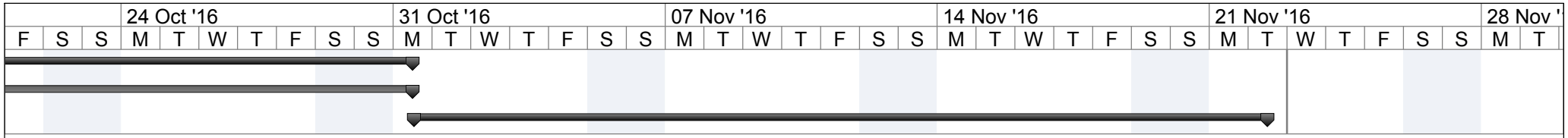
Project: IM MS PLan Access P
Date: Thu 17/12/15

Task	External Milestone	Manual Summary Rollup
Split	Inactive Task	Manual Summary
Milestone	Inactive Milestone	Start-only
Summary	Inactive Summary	Finish-only
Project Summary	Manual Task	Deadline
External Tasks	Duration-only	Progress



Project: IM MS PLan Access P
Date: Thu 17/12/15

Task		External Milestone		Manual Summary Rollup	
Split		Inactive Task		Manual Summary	
Milestone		Inactive Milestone		Start-only	
Summary		Inactive Summary		Finish-only	
Project Summary		Manual Task		Deadline	
External Tasks		Duration-only		Progress	



Project: IM MS PLan Access P
Date: Thu 17/12/15

Task	External Milestone	Manual Summary Rollup
Split	Inactive Task	Manual Summary
Milestone	Inactive Milestone	Start-only
Summary	Inactive Summary	Finish-only
Project Summary	Manual Task	Deadline
External Tasks	Duration-only	Progress

APPENDIX H

Information Security Policy

TfL Standard Information Security

Information Security Controls Framework

Transport for London

Information Security Policy

Issue date: 16 December 2009

Effective: 1 January 2010

This supersedes any previous policy.

Purpose

1. The objective of this policy is to ensure that all the Information Transport for London (TfL) holds in order to deliver its services and operations is managed with appropriate regard for Information Security, so as to:
   (a) Protect its integrity, availability, and confidentiality;
   (b) Minimise the potential consequences of information security breaches by preventing their occurrence in the first instance, or where necessary, containing and reducing their impact; and
   (c) Ensure that personal data is afforded the protection required by the Data Protection Act 1998.
2. This policy applies to all Information held by TfL in any form or medium, electronic, paper or otherwise, including all data held on, or processed by, TfL systems.
3. External service providers must adhere to the principles of this policy; compliance will be monitored through contractual arrangements and audits.

Definitions

4. Information: any information, data or records, irrespective of format, which are generated or used by a business system or process. Examples include electronic communications, emails, video or digital recordings, hard copy (paper) files, images, graphics, maps, plans, technical drawings, programs, software and all other types of data.
5. Information Governance: a business unit within General Counsel.
6. Information Management (IM): a business unit within Finance.
7. Information Owners: senior managers, who are responsible for managing the acquisition, creation, maintenance and disposal of TfL's Information and Information Systems within their assigned area of control.
8. Information Risk: that part of TfL's overall risk portfolio which relates to the, integrity, availability and confidentiality of Information within the TfL Group.

9. Information Security: the ability to protect the integrity, availability, and confidentiality of Information held by TfL and to protect Information from unauthorised use, modification, accidental or intentional damage or destruction.

10. Information Security Breach: an Information Security Incident where it is confirmed that a stated organisational policy or legal requirement regarding Information Security has been contravened.

11. Information Security Incident: a single or a series of unwanted or unexpected Information Security events that have a significant probability of compromising business operations and threatening information security.

12. Information System: Information in all media, hardware, software and supporting networks and the processes and human resources that support its acquisition, storage and communication.

13. Internal Audit: a business unit within General Counsel.

14. TfL Personnel: includes all TfL employees as well as all temporary staff, contractors, consultants and any third parties with whom special arrangements (such as confidentiality and non-disclosure agreements) have been made.

14. Transport for London (TfL): the statutory corporation and its operating subsidiaries.

Organisational scope

15. This policy applies to TfL and to any commercial organisations or service providers (including agencies or consultancy companies) contracted to carry out work for TfL.

Policy statement

14. TfL depends on Information and Information Systems to support and develop its key business objectives, including the provision of public transport services and the implementation of the Mayor of London's Transport Strategy. TfL will adopt appropriate technical and organisational arrangements in accordance with this policy to protect the resilience, integrity, availability and confidentiality of the Information it holds (including personal data relating to both customers and employees) and the systems in which the Information resides.

15. This policy has been developed with reference to the following best practice standards and guidance:

    (a) Information Security Standard ISO/IEC 27001 and associated Code of Practice for Information Security ISO/IEC 27002:2005.

    (b) Her Majesty's Government (HMG) Security Policy Framework.

    (c) Cross Government Mandatory Minimum Measures for Data Handling.

    (d) Government Protective Marking Scheme (GPMS).

    (e) Payment Card Industry Data Security Standard (PCI DSS).

Policy content

16. TfL's policy is to ensure that:

    (a) Information Security is considered as a fundamental and integral part of all TfL operations.

    (b) Statutory requirements to safeguard the security of Information are met and the accuracy, completeness and segregation of personal data are assured.

    (c) Information is accessible to authorised users when they need it and is assigned an appropriate security classification.

    (d) ICT systems, networks and other key infrastructure components are protected from harm and the integrity of Information is maintained and protected from attack and unauthorised access or alteration.

    (e) Information Risk will be considered and afforded a priority in decisions within TfL in the same way as financial and operational risk. This will be reflected in corporate and local risk registers. Information Risk will be managed by a process of identifying, controlling, minimising and/or eliminating risks that may affect TfL's information or information systems.

    (f) Business continuity plans, including disaster recovery plans, are implemented to support business needs and appropriate Information Security training is given to TfL Personnel.

    (g) All Information Security Breaches, actual or suspected, are reported and investigated and a culture exists where improving Information Security procedures is encouraged.

    (h) All necessary measures are taken in order to comply with the Payment Card Industry Data Security Standards (PCI DSS), which are mandatory for organisations processing payment card transactions.

Responsibility for Information Security

17. Each TfL employee is responsible for actively supporting this policy and must ensure that their use of TfL's Information or Information Systems is in accordance with it. Employees must seek advice in the event of uncertainty in relation to this issue.

18. All Cost Centre and Project managers are directly responsible for the security of Information within their business areas.

19. Information Owners are responsible for ensuring that TfL Personnel within their area of control are aware of this policy and are adequately trained in Information Security.

20. Information Owners are responsible for the assessment and reporting of Information Risk within each business unit.

21. Information Owners will define and document relevant statutory and contractual requirements for Information Systems.

22. Information Owners will implement appropriate procedures to ensure compliance with legal restrictions on the use of material in respect of which there may be intellectual property rights including copyright, design rights and trademarks.

23. Information Owners, with support from TfL Personnel who lead on business continuity planning within the relevant business area, will manage and co-ordinate strategies for resilience, including business recovery following information loss or corruption or unauthorised disclosure or access.

24. TfL Personnel who lead on business continuity planning within their business area are responsible for co-ordinating the creation and maintenance of business continuity plans for all departments across TfL, which take account of the requirements of this policy where appropriate.

25. Information Governance, Internal Audit and IM are responsible for managing actual or suspected Information Security Incidents and Breaches and recommending additional or improved security measures to prevent their reoccurrence.

26. Information Governance is responsible for the interpretation of this policy, for monitoring compliance with the policy and for providing advice and guidance on its implementation.

27. IM are responsible for advising the business on the technical measures required to implement this policy and for their implementation on TfL's Information Systems and for ensuring that appropriate technical measures are in place to protect the security of electronic Information.

Procedures/Guidelines/Processes

28. All Information held by TfL must be managed in accordance with TfL's Privacy and Data Protection Policy, Information and Records Management Policy and Information Access Policy.

29. Appropriate Information Security procedures and TfL Standards will be implemented in support of this policy. These will include Standards and procedures as listed in the Annex to this Policy.

30. TfL will have in place an Information Security Classification Standard for protectively marking Information. Security classifications will be applied to all of TfL's Information on creation or receipt, irrespective of format or medium, and Information classified according to this Standard must be transmitted, stored and disposed of as required by the classification Standard and its accompanying instructions.

31. TfL personnel handling Information which has been protectively marked in accordance with HMG's Security Policy Framework (SPF) will adhere to the requirements of the SPF.

32. Actual or suspected Information Security Incidents involving personal or sensitive personal data (as defined by the Data Protection Act 1998) must be reported to Information Governance in order for the incident to be managed in accordance with the Incident Management Procedure for the Loss or Unauthorised Disclosure of Personal Data.

33. Internal Audit will perform a periodic audit of the security processes, procedures and practices of TfL and its service providers to monitor compliance with this policy.

Approval and amendments

34. This policy was approved by the Commissioner on 18 November 2009.

35. This policy was approved by the Audit Committee on 16 December 2009.

36. Following an organisational restructure, a number of minor amendments to this Policy were made on 2 May 2012.

37. This policy will be subject to periodic review as considered appropriate by General Counsel.

Policy owner

38. TfL's General Counsel is the designated owner of this policy.

Annex: Information Security Standards and procedures

Standards and procedures covering the following topics will be implemented in support of the Information Security Policy:

- Physical security of data centres, communications rooms and sensitive zones.
- Incident management.
- Business continuity.
- CMDB (IT asset register).
- Security vetting for sensitive roles within Information Management (IM).
- IT user registration.
- Back-up.
- Cryptographic controls.
- Third party connections.
- Change management.
- Development and test areas.
- Access controls.
- System requirements analysis.
- Mobile computing and remote working.
- Input data validation.
- Integrity of software and information.
- Acceptable use and user responsibilities.
- Information handling.

Transport for London

TfL Standard – Information Security Classification

Issue date: 1 July 2010
Effective: 1 July 2010

Table of contents

Part 1: TfL Information Security Classification Standard

Purpose

1. This TfL Standard sets out an information security classification scheme covering information and records, in all formats, held by TfL. The objectives are to:
   (a) Improve the reliability of, and confidence in, the security of our stored information.
   (b) Reduce information risk, including the likelihood of security incidents or data breaches.
   (c) Clarify the categories of information which require secure handling.
   (d) Reduce the burden of determining which information requires secure handling.
2. The Standard is designed to:
   (a) Provide clear guidelines to all TfL Personnel on minimum security standards for the information they manage.
   (b) Provide a set of standard requirements for managing information in accordance with its defined security classification.
   (c) Provide a set of classifications which TfL Personnel must use when labelling unpublished information.

Definitions

3. Information: any information, data or records, irrespective of format, generated or used by a business system or process. Examples include electronic communications, emails, video or digital recordings, hard copy (paper) files, images, graphics, maps, plans and technical drawings.
4. Information Classification: assigning a piece of information to a particular category depending on its content.
5. Information Owners: senior managers, who are responsible for managing the acquisition, creation, maintenance and disposal of TfL's Information and Information Systems within their assigned area of control.
6. Information Risk: that part of TfL's overall risk portfolio which relates to the integrity, availability and confidentiality of Information within TfL.
7. Information Security: the ability to protect the integrity, availability, and confidentiality of information held by TfL and to protect information from unauthorised use, disclosure, modification, accidental or intentional damage or destruction.
8. Information Security Breach: an Information Security Incident where it is confirmed that a stated organisational policy or legal requirement regarding Information Security has been contravened.

9. Information Security Incident: a single or a series of unwanted or unexpected Information Security events that have a significant probability of compromising business operations and threatening information security.

10. Information System: information in all media, hardware, software and supporting networks and the processes and human resources that support its acquisition, storage and communication.

11. Records: information captured in either paper or electronic format and held by an organisation (or person), in pursuance of their activities, business transactions or legal obligations.

12. Secure: an adjective used in this document to define the requirement to manage information in such a way as to minimise the risk of a Security Incident occurring through unauthorised disclosure of or access to information.

13. Transport for London (TfL): the statutory corporation and its operating subsidiaries.

14. TfL Personnel: includes all TfL employees as well as all temporary staff, contractors, consultants and any third parties with whom special arrangements (such as confidentiality and non-disclosure agreements) have been made.

Scope

15. This Standard is consistent with TfL's information governance policies (including but not limited to the Information Security Policy; Information and Records Management Policy; and Privacy and Data Protection Policy).

16. The Standard also complies with the requirements of the Payment Card Industry Data Security Standard (PCI DSS) and the Data Protection Act 1998 covering the secure storage and transmission of data.

17. The classification scheme outlined in this Standard does not apply to information received by TfL which is protectively marked in accordance with the Government Security Classification Policy issued by the Cabinet Office. Such information must be managed in accordance with the Government Security Classification Policy. Detailed guidance on data handling in accordance with that Policy will be made available to TfL Personnel who handle such information.

18. The provisions of this Standard will not, as a rule, be applied retrospectively but will come into force from the date on which the Standard is issued.

19. The Standard includes:

    (a) A description of the classes of information which require protective marking for security purposes.

    (b) Notes on the potential impact on TfL of accidental or deliberate compromise of the various classes of information.

    (c) Examples of information covered by each security classification.

    (d) Summary guidance on the storage, circulation and disposal of the various classes of information. More detailed requirements for the secure handling of information are included in the Appendix to this Standard.

Roles and responsibilities

20. TfL will implement all necessary measures to protect the security of information in all formats.
21. TfL's Information Owners are responsible for ensuring that TfL Personnel comply with the procedures outlined in the Standard and with relevant information governance policies.
22. Information Governance is responsible, in consultation with the business, for maintaining this Standard and other corporate Policies/Standards relating to information and records management and producing general guidance on best practice in the management and disposal of information and records**.**
23. Information Management (IM) is responsible for ensuring that TfL's Information Systems are capable of meeting the security/handling requirements associated with the security classification of information processed or stored on them.
24. The TfL Records Management Stakeholder Network is responsible for disseminating advice and guidance on best practice in information security and records management.
25. All TfL Personnel are responsible for managing information responsibly and in accordance with TfL's information governance policies, standards and procedures. This includes responsibility for assigning a security classification to information they produce or create and storing and processing it in accordance with Part 2 of this Standard.

Procedures and processes

26. Any new or revised procedure or process developed by TfL which refers to the creation and processing of information should make reference to this Standard and explicitly address the need to classify the associated information in accordance with the security classification scheme detailed in Part 2.

Approval

27. This Standard was approved at the meeting of the TfL Leadership Team on 22 March 2010.
28. This Standard will be subject to periodic review as considered appropriate by General Counsel.
29. Following an organisational restructure, a number of minor amendments to this Standard were made on 22 May 2012.
30. The Standard was updated on 1 September 2014 to reflect changes to the name of the Government Security Classification Policy.

Part 2: TfL Information Security Classification Scheme

Note: there is no automatic link between a security classification and an exemption under the Freedom of Information Act (FOIA) or the Environmental Information Regulations (EIRs). A security classification of TfL RESTRICTED or above will be taken into consideration when determining whether an exemption should be applied, but other factors will also affect the outcome of that decision.

Classification: **TfL UNCLASSIFIED**			
Classification description	**Impact on TfL of accidental or deliberate compromise**	**Examples of information covered by security classification**	**Storage and circulation of information**
Information which: ▪ Could be accessed by any employee of TfL. ▪ Is accessible to TfL customers and the general public. ▪ Where not already publicly available, will as a general rule be provided in response to a request under the FOIA or the EIRs	None.	▪ All material on the websites of TfL and its subsidiary companies. ▪ All material listed in TfL's FOI Publication Schemes. ▪ Published material and archival records held in the TfL Corporate Archives which are classified as open to the public. ▪ All material on Source unless specifically classified as *TfL RESTRICTED* or above. ▪ Corporate policies once approved. ▪ All e-mails and similar electronic messaging technologies other than those classified as *TfL RESTRICTED* or above. ▪ All documents in network shared drives or SharePoint other than those classified as *TfL Restricted* or above. ▪ All information in corporate databases unless classified as *TfL RESTRICTED* or above.	Open access storage and circulation permitted, other than for original material in the Archives which may only be viewed on site (copies may be made available on request).

Classification: **TfL RESTRICTED** (all information other than personal data)			
Classification description	**Impact on TfL of accidental or deliberate compromise**	**Examples of information covered by security classification**	**Storage and circulation of information**
Restricted for a specified period of time to authorised persons. Security status will as a general rule be downgraded to "*TfL UNCLASSIFIED*" after a set period of time, ie once no adverse impact would result from disclosure, based on a risk assessment (eg once a policy is approved and published). If known, this should be recorded alongside the classification. Information may be provided to the general public under the FOIA or the EIRs provided it is first de-classified (after a decision has been made not to apply an exemption under the FOIA or EIRs).	**Medium -** Risk of: ▪ causing financial loss or loss of earning potential or facilitating improper gain or advantage for individuals or companies; ▪ disadvantage in commercial or policy negotiations with others; ▪ undermining the proper management and operations of TfL or other public bodies; ▪ prejudicing the investigation or facilitating the commission of crime; ▪ impeding the effective development or operation of TfL policies, or those of other public bodies; ▪ causing disruption of a number of key transport systems for up to 24 hours.	▪ Commercial eg contracts. ▪ Minutes and papers of closed meetings of the TfL Board, its Committees and Panels. ▪ Management of departmental finances and staff. ▪ Risk management and business continuity plans. ▪ Policy development where availability could prejudice the free and frank exchange of ideas or views. ▪ Information provided under an express or implied guarantee of confidentiality. ▪ Investigations into suspected criminal offences (other than systemic fraud or serious crimes). ▪ Discovered material in relation to litigation unless used or referred to in court. ▪ Information relevant to on-going legal cases where unauthorised disclosure could prejudice the conduct of the case. ▪ Any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.	Secure storage and a clear desk policy; within shared systems must be restricted to those with authorised access and be given protection from unauthorised access/alteration. Should be processed, transmitted and disposed of securely. It is acceptable to transmit information via email and similar electronic messaging technologies, external or internal post.

Classification: **TfL RESTRICTED** (‘personal data’)			
Classification description	**Impact on TfL of accidental or deliberate compromise**	**Examples of information covered by security classification**	**Storage and circulation of information**
Restricted to authorised persons. Includes personal data and sensitive personal data, as defined by the Data Protection Act 1998, regarding employees, customers and the general public; will be provided to the data subject in response to a subject access request. Security status of personal data will not change until the death of the data subject.	**Medium -** Risk of (continued): ▪ causing distress to individuals; ▪ breach of statutory restrictions on the disclosure of information; ▪ breach of proper undertakings to maintain the confidence of information provided by third parties.	▪ Data about a living individual which is essentially of a biographical nature eg: - Personal contact details. - Bank account details. - Personal comments about an individual. - Oyster journey history data. ▪ Employee records, including: - Staff interview or counselling records. - Redundancy records. - Sick pay records. - Maternity pay records. - Income tax and National Insurance returns. - Salary/pension records. ▪ Sensitive personal data, including information about: - Racial or ethnic origins. - Political opinions. - Religious beliefs or other beliefs of a similar nature. - Trade union membership. - Physical or mental health or condition. - Sexual life.	Secure storage and a clear desk policy; within shared systems must be restricted to those with authorised access and be given protection from unauthorised access/alteration. Should be processed, transmitted and disposed of securely. Sensitive personal data or data relating to an individual’s finances should not be transmitted via email or similar electronic messaging technologies unless encrypted. It is acceptable to transmit other personal data via a TfL email account, external or internal post. Internal post should be sealed. Personal data should only be stored on a USB stick or other removable media if the data and/or device has been encrypted.

Classification: **TfL CONFIDENTIAL**			
Classification description	**Impact on TfL of accidental or deliberate compromise**	**Examples of information covered by security classification**	**Storage and circulation of information**
Restricted for extended periods of time to authorised persons only.	**High -** Significant risk of: ▪ Prejudice to individual security or liberty; ▪ Impeding the investigation or facilitating the commission of serious crime; ▪ Shutting down or otherwise substantially disrupting significant national operations including London's transport infrastructure; ▪ Substantially undermining the financial viability of TfL or other major organisations; ▪ Working substantially against national finances or economic and commercial interests; ▪ Seriously impeding the development or operation of major central/local government policies.	▪ Third party intelligence, information or allegations provided under an express guarantee of confidentiality, relating to alleged or actual criminal activity, including fraud. ▪ Details of current or recent criminal investigations of serious offences or systemic fraud. ▪ IT security procedures. ▪ Building security procedures. ▪ Personnel security procedures. ▪ Documents where release would compromise TfL's ability to safely operate transport services. ▪ Transport infrastructure records eg technical plans and specifications. ▪ Operational disaster plans eg evacuation procedures. ▪ Debit or credit cardholder data comprising a Primary Account Number (PAN) and (if stored in conjunction with the PAN), the cardholder name, service code or expiration date.	Secure storage (locked filing cabinets or safes and rooms) for paper records; shared systems must be restricted to those with authorised access and be given protection from unauthorised access/alteration. Must be processed, transmitted and disposed of securely. Must not be stored on a USB stick or other removable media, unless both the data and device are adequately encrypted. Must not be transmitted via email or any other electronic messaging technologies unless encrypted. Must be transmitted by post in double envelopes (both sealed): externally via registered mail or courier; internally, by hand direct to the intended recipient.

APPENDIX

TfL Requirements for the Secure Handling of Information

Issue date: 21 December 2010

Effective: 1 February 2011

These requirements have been produced by Information Governance to support compliance with TfL's Information Security Classification Standard. They provide clear guidance on the appropriate handling of information based on the security classification allocated to that information.

Table of contents

1. Key to terms used

Electronic messaging technologies: include email, Office Communicator, Blackberry Messenger.

Information Owners: senior managers, who are responsible for managing the acquisition, creation, maintenance and disposal of TfL's information and information systems within their assigned area of control.

Mobile computing devices: laptops, Blackberrys, PDAs and similar devices.

Removable storage media: include microfilm, CDR, DVD, USB, magnetic tapes, disks, removable hard drives.

Shared systems: include shared network drives, TfL Document Manager, SharePoint sites, all other TfL databases.

2. TfL information security classification labels

- TfL UNCLASSIFIED: no security marking necessary
- TfL RESTRICTED: security marking as specified in this document
- TfL CONFIDENTIAL: security marking as specified in this document

These labels are described in greater detail in TfL's Information Security Classification Standard.

3. Descriptors

Descriptors are additional descriptive terms appended to the main classification label in order to clarify why a particular classification has been assigned eg 'TfL RESTRICTED – CUSTOMER DATA'; 'TfL RESTRICTED – POLICY. Use of descriptors is optional and may be tailored to the requirements of the individual business area.

4. Re-assigning information security classifications

- The information security classifications described in this document are indicative of the sensitivity or otherwise of TfL information and may change over time.
- Re-assigning classifications will occur quite commonly where information is only sensitive for a limited time eg once a policy is approved, or a contract is awarded following a procurement exercise.
- Government information classified under the Government Security Classification Policy will retain that classification and be treated in accordance with the relevant handling requirements issued by the Cabinet Office.
- Information from other organisations (except those which use the Government Security Classification Policy) marked 'Confidential' will by default be labelled 'TfL RESTRICTED' unless otherwise agreed in writing (for example in a contract, information sharing agreement, or Code of Connection).

5. Retrospective application

TfL information security classifications do not have to be applied retrospectively (ie to legacy information) other than to information which is re-activated for current business use.

6. Where to apply labels to information

Application	System administrator to add to metadata
Database	System administrator to add label to the login screen or as a banner within the database
Electronic Document Management System (EDMS)	System administrator to apply labels in metadata
SharePoint	Administrator to apply labels to individual sites or in document library metadata; where this is not appropriate the Administrator must mandate the application of labels by users (ie to individual documents)
File system	Information Owner or user to apply labels as appropriate: ▪ Electronic folder names – use highest level classification applicable to any of its contents ▪ Cover of hard copy files/folders – use highest level classification applicable to any of its contents
Documents created electronically	▪ User to add in footer (on every page) and on title page/cover if applicable ▪ 'TfL RESTRICTED' and 'TfL CONFIDENTIAL' options to be added to footer of document templates – user to apply relevant classification and delete as appropriate
Documents created manually	Stamped/noted on every page
Email messages	User to add label at the end of the subject line
Other electronic messaging technologies	User to add classification at beginning of body of text
Removable storage media	User to label the storage device itself plus container, using a permanent marker
Verbal information	Instigator to mention at beginning of, or at the appropriate point in, the conversation

7.1 Handling requirements: TfL UNCLASSIFIED - hard copy information	
Security marking	▪ No security marking necessary
Access	▪ Unrestricted access
Storage	▪ Any eg open shelving, desk top
Transmission/ information sharing	▪ Any storage and circulation permitted ▪ Exception: original unpublished material held in the TfL Corporate Archives which may only be viewed on site by prior arrangement (copies may be made available on request)
Disposal	▪ Any method permitted

7.2 Handling requirements: TfL UNCLASSIFIED - electronic information	
Security marking	▪ No security marking necessary
Access	▪ Unrestricted access
Storage	▪ Any information storage system which has been approved by IM for use within TfL
Transmission/ information sharing	▪ Any storage and circulation permitted
Disposal	▪ Any method permitted

8.1 Handling requirements: TfL RESTRICTED - hard copy information	
Security marking	▪ Add security label to cover of file (a stamp marked 'TfL RESTRICTED' is recommended) ▪ If a file/folder contains any information which is 'TfL RESTRICTED' the entire file/folder will need to be marked 'TfL RESTRICTED' ▪ Add security label to individual documents (stamp/note on every page) unless the document is a hard copy of an electronically generated internal document and already has the marking in the footer
Access	▪ Filing systems to have a designated Information Owner responsible for authorising and monitoring access ▪ Restricted to authorised persons ▪ Access should be reviewed by Information Owners on a regular basis ▪ Where access is granted to a third party outside the business, the Information Owner must ensure that a non-disclosure/confidentiality agreement is in place ▪ If accessed in a public place, ensure the information cannot be viewed by others
Storage	▪ To be stored in shelving/cabinets/drawers which are locked when not in use ▪ Not to be left on desks when unattended for long periods or overnight (clear desk policy)
Transmission/ information sharing	▪ Must not be removed from TfL premises unless authorised by the Information Owner(s) ▪ May be transmitted via external or internal post or fax ▪ Photocopies or originals may be shared with authorised persons ▪ If shared by telephone identity of recipient should be established to ensure they are authorised to access the information ▪ May be scanned into a secure storage system (ie which has been approved by IM Security as having the requisite level of security to handle 'TfL RESTRICTED' information) by users authorised to access that system ▪ Faxes should only be used to transmit personal information where the security status of the receiving machine is assured and the recipient is on standby to receive the fax ▪ Sensitive personal information or information relating to an individual's finances should not be transmitted via fax unless an encrypted fax service is available
Disposal	▪ Non-current 'TfL RESTRICTED' information which needs to be kept for a specified period prior to destruction (eg in accordance with TfL's Information and Records Disposal Schedule) should be either held in a secure on-site area or transferred to a TfL approved external records store where it will be protected through controlled access to the area and a secure physical environment ▪ Must be shredded or placed in security shredding bin ▪ Information to be erased from whiteboards and removed from flip charts and shredded

8.2 Handling requirements: TfL RESTRICTED - electronic information	
Security marking	▪ Documents: add security label 'TfL RESTRICTED' in footer (uppercase Arial, 12 point font) ▪ Excel spreadsheets: add security label 'TfL RESTRICTED' below title ▪ Emails: add security label 'TfL RESTRICTED' at end of the subject line and separated by a hyphen ▪ Other electronic messaging technologies: add security label 'TfL RESTRICTED' at the beginning of the body of the text ▪ Shared systems and databases: where it is not possible to label individual records within a database or system then the whole database or system should be assigned the classification level eg by adding the label to the login screen or having it as a banner within the database/system ▪ DVD/CDR/magnetic tapes - user to label the storage device and container 'TfL RESTRICTED'
Access	▪ Each application or system to have a designated Information Owner responsible for authorising and monitoring access ▪ Shared systems: restricted to those authorised to view 'TfL RESTRICTED' information and protected from unauthorised access/alteration ▪ User access permissions for relevant systems must be clearly documented and regularly reviewed/updated ▪ Where access is granted to a third party outside the business, the Information Owner must ensure that a non-disclosure/confidentiality agreement is in place ▪ Mobile computing devices must be password or pin protected ▪ PCs and mobile computing devices must be locked, logged off the network or shut down when unattended ▪ If accessed in a public place via a mobile computing device, ensure the information cannot be viewed by others
Storage	▪ Any secure information storage system (ie which has been approved by IM Security as having the requisite level of security to handle 'TfL RESTRICTED' information) ▪ Personal data must only be stored on a mobile computing device, USB stick or other removable media if the data and/or device has been adequately encrypted ▪ All removable storage media should be stored in a locked secure cabinet when not in use
Transmission/ information sharing	▪ If shared by telephone identity of recipient should be established to ensure they are authorised to access the data ▪ Do not send unencrypted email containing personal information unless absolutely unavoidable and then only within the tfl.gov.uk network ▪ May be shared with authorised external users via encrypted email or using an IM approved secure network connection eg VPN or SSL ▪ Email attachments containing personal information should, as a minimum, be winzipped for extra security ▪ If printed, must be collected immediately, unless using a secure device which is swipe card or PIN activated
Disposal	▪ Individuals responsible for disposal must ensure that all media formats are disposed of appropriately and that no duplicate information remains ▪ Removable storage media containing 'TfL RESTRICTED' information must be passed to IM for secure disposal ▪ 'TfL RESTRICTED' information in corporate systems must be disposed of securely by IM in such a way as to ensure that it cannot be reconstituted

9.1 Handling requirements: TfL CONFIDENTIAL - hard copy information	
Security marking	▪ Add security label to cover of file (a stamp marked 'TfL CONFIDENTIAL' is recommended) ▪ If a file/folder contains any information which is 'TfL CONFIDENTIAL' the entire file/folder will need to be marked 'TfL CONFIDENTIAL' ▪ Add security label to individual documents (stamp/note on every page) unless the document is a hard copy of an electronically generated internal document and already has the marking in the footer
Access	▪ Filing systems to have a designated Information Owner responsible for authorising and monitoring access ▪ Restricted to authorised users as determined by the Information Owner ▪ A list of persons authorised to access and/or maintain 'TfL CONFIDENTIAL' information should be kept and reviewed regularly by Information Owners ▪ Appropriate security screening (to be defined by the relevant business area in consultation with HR) is required for individuals who are employed in posts which require regular access to 'TfL CONFIDENTIAL' information ▪ Where access is granted to a third party outside the business, the Information Owner must ensure that a non-disclosure/confidentiality agreement is in place ▪ Must not be accessed in a public place (eg a train, cafe)
Storage	▪ Locked filing cabinets or safes within locked and password controlled rooms ▪ Storage areas containing 'TfL CONFIDENTIAL' information should be locked at all times when not in use ▪ Clear desk policy mandatory whenever workstation unattended
Transmission/ information sharing	▪ Must not be removed from TfL premises by users unless authorised by the Information Owner ▪ Must be transmitted externally via registered mail or courier in double envelopes (both sealed) ▪ Must be transmitted internally by hand direct to the intended recipient double enveloped with security marking on inner envelope ▪ May be scanned into a secure storage system (ie which has been approved by IM Security as having the requisite level of security to handle 'TfL CONFIDENTIAL' information) by users authorised to access that system ▪ Faxes should not be used unless an encrypted fax service is available and the recipient is on standby to receive the fax ▪ Should not be photocopied unless the user's account is password protected
Disposal	▪ Non-current 'TfL CONFIDENTIAL' information which needs to be kept for a specified period prior to destruction (eg in accordance with TfL's Information and Records Disposal Schedule) must be either held in a secure on-site area or sealed with security tags and transferred to a TfL approved external records store where it will be protected through controlled access to the area and a secure physical environment ▪ Must be shredded or placed in security shredding bin ▪ Information must be erased from whiteboards and removed from flip charts and shredded

9.2 Handling requirements: TfL CONFIDENTIAL - electronic information	
Security marking	▪ Documents: add security label 'TfL CONFIDENTIAL' in footer (uppercase Arial, 12 point font) ▪ Excel spreadsheets: add security label 'TfL CONFIDENTIAL' below title ▪ Emails: all emails in this category will be encrypted but should also include the security marking 'TfL CONFIDENTIAL' at the end of the subject line and separated by a hyphen as an extra security measure ▪ Other electronic messaging technologies: will be encrypted but should also include the security marking 'TfL CONFIDENTIAL' at the beginning of the body of the text ▪ Shared systems: all information in a shared system designated as 'TfL CONFIDENTIAL' will inherit that classification ▪ DVD/CDR/magnetic tapes - user to label the storage device and container 'TfL CONFIDENTIAL'
Access	▪ Each application or system to have a designated Information Owner responsible for authorising and monitoring access ▪ Shared systems: restricted to those authorised to view 'TfL CONFIDENTIAL' information ▪ User access permissions for relevant systems must be clearly documented and regularly reviewed/updated ▪ A list of persons authorised to access and/or maintain information designated 'TfL CONFIDENTIAL' must be kept and reviewed regularly by Information Owners (for their assigned area of control) ▪ Appropriate security screening (to be defined by the relevant business area in consultation with HR) is required for individuals who are employed in posts which require regular access to 'TfL CONFIDENTIAL' information ▪ Mobile computing devices must be password or PIN protected ▪ PCs and mobile computing devices must be locked, logged off the network or shut down when unattended ▪ Where access is granted to a third party outside the business, the Information Owner must ensure that a non-disclosure/confidentiality agreement is in place ▪ Must not be accessed via a mobile computing device in a public place (eg a train, internet cafe)
Storage	▪ A secure storage system (ie which has been approved by IM Security as having the requisite level of security to handle 'TfL CONFIDENTIAL' information) ▪ Must not be stored on removable storage media unless both the data and device are adequately encrypted ▪ Data accessed remotely must not be transferred to external hard drives or removable storage media ▪ All removable storage media must be stored in a locked secure cabinets (or safe) within a locked room
Transmission/ information sharing	▪ Where information is held outside the source system it must be encrypted ▪ May only be transmitted via telephone in cases of operational emergency ▪ Must not be transmitted via email or similar electronic messaging technologies unless encrypted ▪ If printed, must be collected immediately, unless using a secure device which is swipe card or PIN activated ▪ May only be shared with external agencies/across open public networks via a secure encrypted network connection
Disposal	▪ Information Owners are responsible for ensuring that all media formats/duplicate copies are disposed of appropriately ▪ Removable storage media containing 'TfL CONFIDENTIAL' information must be passed to IM by the Information Owner for secure disposal by triple overwriting or disintegration ▪ 'TfL CONFIDENTIAL' information in corporate systems, backup tapes and hard drives must be disposed of securely by IM so as to ensure that it cannot be reconstituted

Reference Document

IM-RD-SD6.0-001

Information Security Controls Framework

MAYOR OF LONDON

Transport for London

Contents

1 Purpose

"Information is a valuable TfL resource and shall be protected. The TfL Information Security Controls Framework (ISCF) describes the requirements and approaches that will be applied to protect our information assets. This is a central repository for information security controls, and enables a traceable, repeatable and testable set of security requirements."

Chief Information Security Officer (CISO)

This document will:

- Detail traceable, repeatable and testable security controls to protect TfL's information systems;
- Detail the information security requirements (there are 171 in total) of Information Owners responsible for operating business processes which handle information;
- Serve as the foundation for all derived information security documents;
- Provide a baseline of security controls that can be used to measure compliance;
- Provide a detailed set of security requirements that can form contractual obligations for suppliers processing TfL information;
- Serve as the security controls requirements for all cyber systems;
- Provide the required traceability to the HMG Security Policy Framework.

2 Scope

Our primary goal remains to "keep London working and growing, and make life in London better." This includes keeping our information secure, whilst providing value through appropriate access and availability of information ensuring business targets are met. Information security is the holistic view of how we value, use, store and protect information. The TfL Information Security Controls Framework is a central repository of information security controls for TfL, and is aligned with Her Majesty's Government (HMG) Security Policy Framework, the SANS 20 Critical controls, Payment Card Industry and Data Security Standard (PCI-DSS) and TfL unique controls.

There are two main categories of controls in this document:

a) **Technical Controls** – controls implemented and maintained by Information Security technical team;

b) **Nontechnical Controls** – controls normally implemented by business line managers who are responsible for operating TfL business processes. These controls will form the basis for Security Policy as applicable to employees and suppliers e.g. Acceptable Use, Third Party usage.

This framework applies to all activities and services within the remit of IM and shall be adopted accordingly as changes are made to existing services or new services are provided. It should be considered good practice elsewhere within the business for activities and services outside of IM's direct control and it is envisaged that this framework will be promoted to mandatory requirements for these subject to gaining approval via the TfL Change Team.

This Framework is maintained by the IM Chief Information Security Officer (CISO) and has been subject to full review and approval by the appropriate governance bodies within

Information Management (IM). It shall be implemented by the appropriate information security team member, or business manager. Future changes to this document are subject to full IM governance rigour.

3 Information Security Controls

The security controls protect information assets by strengthening TfL's defensive posture through continuous and sometimes automated protection and monitoring of the information technology infrastructure to reduce compromises, minimise the need for recovery efforts and provide necessary segregation and lower associated costs. The controls are listed below:

#	Nontechnical	Technical	Controls
1		✓	Inventory Of Authorised and Unauthorised Devices
2		✓	Inventory of Authorised and Unauthorised Software
3		✓	Configuration Control
4		✓	Vulnerability Assessment and Remediation
5		✓	Malware Protection, Detection and Elimination
6		✓	Application Software Security
7		✓	Wireless Device Control
8		✓	Data backup and Recovery
9	✓		Security Skills and Upkeep
10	✓	✓	Regulatory Alignment
11		✓	Network Device Security
12		✓	Network ports, processes and services control
13	✓	✓	Administrative Privileges
14		✓	Network Boundary Defense
15		✓	Audit Log Process
16	✓		Classification of Information
17		✓	Account Control
18	✓	✓	Data Loss Prevention
19	✓	✓	Incident management
20		✓	Lockdown Network Control
21		✓	Penetration Testing
22		✓	Compliance Monitoring
23		✓	Exception Control
24		✓	Physical Security
25		✓	Encryption
26		✓	Policy Maintenance
27	✓	✓	Information Disposal
28	✓	✓	Third Party Computing
29	✓		Information Asset Register

Table 1 – Nontechnical and Technical Controls

3.1 Inventory of Authorised and Unauthorised Devices

3.1.1 Definition:

The processes and tools used to track/control/prevent/correct installation and execution of software on computers based on an asset inventory of approved software.

3.1.2 Requirement:

a. TfL shall develop an inventory of information assets that identifies their critical information and maps critical information to the hardware assets (including servers, workstations, and laptops) on which it is located. A department and/or individual owner responsible for each information asset shall be identified, recorded, and tracked.

b. TfL shall set up an automated asset inventory discovery tool to build an asset inventory of systems connected to TfL public and private network(s). Both active tools that scan through network address ranges and passive tools that identify hosts based on analysing their traffic should be employed.

c. TfL shall set up dynamic host configuration protocol (DHCP) server logging, and utilise a system to improve the asset inventory process. This will aid and help detect unknown systems.

3.2 Inventory of Authorised and Unauthorised Software

3.2.1 Definition:

The processes and tools used to track/control/prevent/correct installation and execution of software on computers based on an asset inventory of approved software.

3.2.2 Requirement:

a. TfL shall set up a white list of technology that can run on the network. This list should be checked for file integrity with automated tools.

b. TfL shall set up an application white listing technology that allows systems to run software only if it is included on the white list and prevents execution of all other software on the system.

c. TfL shall perform regular scanning for unauthorised software and generate alerts when it is discovered on a system. Regular scanning is defined as no less than once a quarter, rotating the day of the week.

d. TfL shall set up software inventory tools covering each of the operating system types in use, including servers, workstations, and mobile devices. The software inventory system shall track the version of the underlying operating system and the applications installed on it. Furthermore, the tool should record not only the type of software installed on each system, but also its version number and patch level. The software inventory should be tied to vulnerability

e. TfL software inventory systems shall be tied into the hardware asset inventory so that all devices and associated software are tracked from a single location.

f. For all TfL developed software TfL shall hold the baseline source code in a password protected database.

3.3 Configuration Control

3.3.1 Definition:

The processes and tools used to track/control/prevent/correct/manage security weaknesses in the configurations of the hardware and software of mobile devices, laptops, workstations, and servers based on a formal configuration management and change control process.

3.3.2 Requirement:

a. TfL shall have a formal configuration management and change control process. The process shall track/control/prevent/correct security weaknesses in the configurations of the hardware and software of mobile devices, laptops, workstations, and servers and any other IT related devices.

b. TfL shall establish, publish and maintain operating system and application standards, including where required hardened build standards Industry-accepted system hardening standards may include, but are not limited to:

- Centre for Internet Security (CIS);
- International Organisation for Standardisation (ISO);
- SysAdmin Audit Network Security (SANS) Institute;
- National Institute of Standards Technology (NIST).

c. TfL software images shall be stored on securely configured servers, with integrity checking tools and change management to ensure that only authorised changes to the images are possible. Alternatively, these master images can be stored in offline machines, air-gapped from the production network.

d. TfL shall implement automated patching tools and processes that ensure highly critical security tested patches are installed within 48 hours of their release for both applications and for operating system software. For mission critical systems patching shall be within 24 hours.

e. TfL shall define and implement full testing of patches to include a back out procedure.

f. TfL shall limit administrative privileges to very few authorised users who have both the knowledge necessary to administer the operating system, application or database, and the business needs to modify the configuration of the underlying operating system. All administrator accounts shall be approved by the Chief of Information Security (CISO).

g. TfL shall set up system configuration management tools that automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals, such as Active Directory for Windows.

3.4 Vulnerability Assessment and Remediation

3.4.1 Definition:

The processes and tools used to detect/prevent/correct security vulnerabilities in the configuration of devices listed and approved in the asset inventory database.

3.4.2 Requirement:

a. TfL shall run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritised lists of the most critical vulnerabilities to each responsible system administrator. In addition to risk scores that compare the effectiveness of system administrators and departments in reducing risk.

b. TfL shall use a dedicated account, associated with the target system, for authenticated vulnerability scans. The account shall be tied to specific machines at specific IP addresses and will only be used by authorised employees. It will not be used for any other activity.

c. TfL shall monitor logs associated with any scanning activity as per the Audit Log Process (control 15). In addition TfL shall correlate event logs with information from vulnerability scans to establish regular activity, and events where an exploit has been used against a part of the network vulnerability.

d. TfL shall deploy automated patch management and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Tested patches shall be applied to all systems including systems that are air gapped.

3.5 Malware Protection, Detection and Elimination

3.5.1 Definition:

The processes and tools used to detect/prevent/correct installation and execution of malicious software on all devices.

3.5.2 Requirement:

a. TfL shall employ automated tools to continuously monitor workstations, servers, and mobile devices for active, up-to-date anti-malware protection with anti-virus, antispyware, personal firewalls, and host-based IPS functions. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers. The endpoint security solution shall include zero-day protection such as network behavioural heuristics.

b. TfL shall use anti-malware software and signature auto-update features or has administrators manually push updates to all machines on a daily basis.

c. TfL shall configure mobile device, workstations, and servers so that they shall not auto-run content from USB tokens (i.e., “thumb drives”), USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, mounted network shares, or other removable media.

d. Limit use of external devices to those that have an authorised business need.

e. TfL shall configure systems so that they conduct an automated anti-malware scan of removable media when it is inserted.

f. TfL shall scan and block all e-mail attachments entering the organisation’s e-mail gateway if they contain malicious code or file types unneeded for the organisation’s

business. This scanning shall be done before the e-mail is placed in the user's inbox. This includes e-mail content filtering and web content filtering.

g. TfL shall apply anti-virus scanning, for inbound and outbound traffic, at the Web Proxy gateway. Content filtering for file-types shall be applied at the perimeter.

h. TfL shall limit/block access to external websites, as identified in the by TfL web filter policy.

3.6 Application Software Security

3.6.1 Definition:

The processes and tools organisations use to detect/prevent/correct security weaknesses in the development and acquisition of software applications.

3.6.2 Requirement:

a. TfL shall deploy web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks, including but not limited to cross-site scripting, SQL injection, command injection, and directory traversal attacks. For applications that are not web-based, specific application firewalls shall be deployed. If traffic is encrypted the device shall either sit behind the encryption or be capable of decrypting the traffic prior to analysis.

b. TfL shall perform vulnerability scans on all Internet-accessible web applications on a weekly basis, alerting or sending e-mail to administrative personnel within 24 hours of completing a scan.

c. TfL shall test in-house-developed and third-party-procured web applications for common security weaknesses using automated remote web application scanners prior to initial deployment, after any major upgrade and on a yearly basis.

d. TfL shall perform explicit error checking for all input. As a minimum when input is provided by the user it shall be verified that it does not exceed the size or the data type of the memory location in which it is stored or moved in the future. Whenever a variable is created in source code, the size and type shall be determined.

e. TfL shall ensure that applications that rely on a database use standard secure configurations (see 3b. Configuration Control) for both the operating system housing the database and the database software itself.

f. TfL shall maintain separate environments for production and non-production systems. Developers shall not have unmonitored access to production environments.

g. Any developer copy/clone of a production database shall be cleansed of confidential/personal record data.

h. TfL shall ensure sample scripts, libraries, components, compilers, or any other unnecessary code that is not being used by an application, is uninstalled or removed from systems.

i. TfL applications shall not display system error messages to end-users.

3.7 Wireless Device Control

3.7.1 Definition:

The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LANS), access points, and wireless client systems.

3.7.2 Requirement:

a. TfL shall maintain an authorised configuration and security profile for each wireless device connected to the network. Devices without the profile shall not be allowed on the wireless internal TfL network.

b. TfL guest wireless shall be for guest use only and maintained per this controls framework.

c. TfL shall ensure any data traversing a wireless network is be secured using a secure wireless protocol. Such as the WPA2 protocol using a new AES-based algorithm, CCMP, which is considered fully secure at this time. Authentication is performed either by the wireless access point (referred to as WPA2-PSK) or by a 3rd party entity such as a Radius server.

d. TfL shall manage all wireless access points using enterprise management tools.

e. TfL shall perform vulnerability scanning to detect wireless access points connected to the wired network, surface and subsurface. Identified devices shall be reconciled against a list of authorised wireless access points.

3.8 Data backup and Recovery

3.8.1 Definition:

The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

3.8.2 Requirement:

a. TfL shall perform an automatic back up on a daily basis. Systems with time sensitive information will be identified and backed up appropriately. Any back up with restricted or confidential information shall follow the guidelines in Section 16.

b. Backups shall be kept offsite and inline with the guidelines in Section 16.

c. TfL shall test the data on backup media on a monthly basis by performing a data restoration process to ensure that the backup is working.

d. TfL shall ensure backups are protected as per the Information Classification Policy.

e. TfL shall train key personal on both the backup and restoration processes.

3.9 Security Skills and Upkeep

3.9.1 Definition:

The process and tools to make sure an organisation understands the technical skill gaps within its workforce, the managerial responsibilities of the information owners including an integrated plan to fill the gaps through policy, training, and awareness.

3.9.2 Requirement:

a. TfL shall perform gap analysis to see which skills employees need and which behaviours employees are not adhering to, using this information to build a training and awareness roadmap. This plan shall be reviewed annually.

b. TfL shall deliver training to fill the skills gap.

c. TfL shall implement an information security awareness program.

d. TfL shall validate and improve awareness levels through periodic tests.

e. TfL shall ensure through awareness training that information data owners are aware of their responsibilities.

f. TfL shall update the IS awareness program in line with environmental changes including the results of compliance checking.

3.10 Regulatory Alignment

3.10.1 Definition:

The processes used to ensure an appropriate level of assurance that regulatory requirements are met.

3.10.2 Requirement:

a. TfL shall have clear policy direction, such as an Acceptable Use Policy, on the use of the systems, applications or devices, so that users know what behaviour is expected of them. Policies shall be communicated frequently and acceptance acknowledged.

b. Noncompliance with Computer Misuse Act or the appropriate regulatory standard may result in prosecution.

c. TfL shall ensure that Personal Data is managed in compliance with the Data Protection Act.

d. TFL shall ensure up to date security policies based on changing EU Legislation, and HMG requirements.

3.11 Network Device Security

3.11.1 Definition:

The processes and tools used to track/control/prevent/correct security weaknesses in the configuration of network devices such as firewalls, routers, and switches based on formal configuration management and change control processes.

3.11.2 Requirement:

a. TfL shall compare each firewall, router, and switch configuration against standard secure configurations (see 3.b Configuration Control) defined for each type of network device in use in the organisation.

b. TfL shall ensure all new configuration rules beyond the standard secure configurations baseline, that allows traffic to flow through network security devices, such as firewalls and network-based IPS, will be documented and recorded in a configuration management system, with a specific business reason for each change, a specific individual's name responsible for that business need, and an expected duration of the need.

c. TfL shall implement ingress and egress filtering at network connections to allow only those ports and protocols with an explicit and documented business need. All other ports and protocols shall be blocked with default-deny rules by firewalls, network-based IPS, and/or routers.

d. TfL shall manage network devices using at least two-factor authentication and encrypted sessions.

e. TfL shall install the latest stable and tested version of any security-related updates within 30 days of the update being released from the device vendor.

3.12 Network ports, processes and services control

3.12.1 Definition:

The processes and tools used to track/control/prevent/correct use of ports, protocols, and services on networked devices.

3.12.2 Requirement:

a. TfL will turn off any service that is not needed for 30 days and after 30 days uninstalled from the system.

b. TfL shall apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

c. TfL shall perform automated port scans on a weekly basis against all key servers and compared to a known effective baseline. If a change that is not listed on the organisation's standard secure configuration is discovered, an alert shall be generated and reviewed by operations.

d. TfL systems shall be capable of identifying any new unauthorised listening network ports that are connected to the network within 24 hours, alerting or sending e-mail notification to a list of enterprise personnel.

3.13 Administrative Privileges

3.13.1 Definition:

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

3.13.2 Requirement:

a. TfL will minimise administrative privileges and accounts. Administrative accounts shall be approved by the Chief of Information Security (CISO). TfL will audit on the use of administrative privileged functions and monitor for anomalous behaviour.

b. TfL shall use automated tools to inventory all administrative accounts monthly, and validate that each person with administrative privileges on desktops, laptops, servers, and WIFI is authorised by the operations manager.

c. TfL shall validate all administrator accounts against AD quarterly, and have line managers review the active list biannually.

d. TfL shall configure all administrative passwords to be complex and contain letters, numbers, and special characters intermixed, with no dictionary words present in the password and so passwords cannot be re-used within a six months timeframe. Admin passwords shall be a minimum of 15 characters.

e. TfL shall ensure all service accounts have long and difficult-to-guess passwords that are changed on a periodic basis, as is done for traditional user and administrative passwords, at a frequent interval of no longer than 90 days. All service accounts shall be approved by IM Security Manager.

f. TfL shall before deploying any new devices in a networked environment, change all default passwords. This includes for applications, operating systems, routers, firewalls, wireless access points, and other systems. Passwords will be held in Password Vault

g. TfL shall store passwords for all systems in a well-hashed or encrypted format, with weaker formats eliminated from the environment. Furthermore, files containing these encrypted or hashed passwords required for systems to authenticate users shall be readable only with super-user privileges.

h. TfL shall utilise access control lists to ensure that administrative accounts are used only for system administration activities, and not for reading e-mail, composing documents, or surfing the Internet. Web browsers and e-mail clients especially shall be configured to never run as administrator.

i. Each person requiring administrative access should be given his/her own separate account. Administrative accounts shall never be shared.

j. Super user accounts shall be approved by the CISO and information owner.

3.14 Network Boundary Defence

3.14.1 Definition:

The processes and tools used to detect/prevent/correct the flow of information transferring Networks of different trust levels with a focus on security damaging data.

3.14.2 Requirement:

a. TfL shall design and implement network perimeters so that all outgoing web, file transfer protocol (FTP), and secure shell traffic to the Internet shall pass through at least one proxy on a DMZ network. The proxy shall support logging individual TCP

sessions; blocking access to specific URLs, domain names, and deny communications with (or limit data flow to) known malicious IP addresses (black lists), or limit access only to trusted sites (white lists).

b. All TfL devices remotely logging into the internal network shall be managed by the enterprise, with remote control of their configuration, installed software, and patch levels.

c. TfL shall periodically scan for back-channel connections to the Internet that bypass the DMZ, including unauthorised VPN connections and dual-homed hosts connected to the enterprise network and to other networks via wireless, dial-up modems, or other mechanisms.

d. On the TfL DMZ networks, the network configuration shall support monitoring systems (which may be built in to the IDS sensors or deployed as a separate technology) to record at least packet header information, and preferably full packet header and payloads of the traffic destined for or passing through the network border.

e. TfL will employ a Security Event Information Management (SEIM) or log analytics system so that events can be correlated from all devices on the network.

f. TfL shall implement the Sender Policy Framework (SPF) by deploying SPF records in DNS and enabling receiver-side verification in mail servers.

g. TfL shall ensure that virtual boundaries e.g. load balancing requirements, shall ensure the appropriate trust levels are employed.

3.15 Audit Log Process

3.15.1 Definition:

The processes and tools used to detect/prevent/correct the use of systems and information based on audit logs of events that are considered significant or could impact the security of an organisation.

3.15.2 Requirement:

a. The audit function shall include at least two synchronised time sources (i.e., Network Time Protocol NTP) from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.

b. TfL shall validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction.

c. TfL shall record logs in a standardised format across the estate.

d. The TfL systems that store logs have adequate storage space for the logs generated on a regular basis, Archive digitally semi-annually.

e. TfL information security shall develop a log retention policy to make sure that the logs are kept for a sufficient period of time.

f. Logs that are restricted or confidential shall be stored IAW section 16.

g. TfL will verbosely log all remote access to a network, whether to the DMZ or the internal network (i.e., VPN, dial-up, or other mechanism).

h. TfL shall log access control events associated with a user attempting to access a resource (e.g., a file or directory) without the appropriate permissions. Failed logon attempts shall also be logged.

i. TfL shall disable leaver accounts, regardless of type, on the day of termination or within 24-hours after termination. This leavers list shall be reconciled against HR leaver list monthly.

j. TfL information security shall have security personnel and/or system administrators run biweekly reports that identify anomalies in logs. They shall then actively review the anomalies, documenting their findings.

k. TfL will secure audit logs so they are not altered. Any changes to audit logs shall generate an alert to IM Security.

l. For the PCI DSS network traffic, examine a sample of audit logs to confirm that the PAN is rendered unreadable or removed from the logs.

m. For PCI DSS network traffic TfL shall implement automated audit trails for all system components to reconstruct the following events:

    1. All individual accesses to cardholder data
    2. All actions taken by any individual with root or administrative privileges
    3. Access to all audit trails
    4. Invalid logical access attempts
    5. Use of identification and authentication mechanisms
    6. Initialisation of the audit logs
    7. Creation and deletion of system-level objects

n. For PCI DSS Network traffic the audit log shall record at least the following audit trail entries for all system components for each event:

    8. User identification
    9. Type of event
    10. Date and time
    11. Success or failure indication
    12. Origination of event
    13. Identity or name of affected data, system component, or resource.

3.16 Classification of Information

3.16.1 Definition:

The processes and tools used to identify/track/control/prevent/correct secure access to information according to the formal determination of which persons, computers, and applications have a need and right to access information based on an approved classification.

3.16.2 Requirement:

a. The classification of information within TfL will be identified and documented by subject matter experts and held within each community. The subject matter expert shall be the information owner.

b. The TfL Security Classification Standard identifies the processes for handling TfL Unclassified, TfL Restricted and TfL Confidential.

3.17 Account Control

3.17.1 Definition:

The processes and tools used to track/control/prevent/correct the use of system and application accounts.

3.17.2 Requirement:

a. TfL shall record and process access requests via the Remedy system.

b. TfL shared drive, SAP, and other storage repositories permissions are reviewed every 90 days by the site owner.

c. TfL shall automatically create a report on a daily basis that includes a list of locked-out accounts, disabled accounts, accounts with passwords that exceed the maximum password age, and accounts with passwords that never expire. This list shall be sent to the associated system administrator in a secure fashion (see Information Classification Protection Requirements for further guidance).

d. TfL will establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor if required.

e. TfL shall require that all non-administrator accounts have strong passwords that contain letters, numbers, and special characters, be changed at least every 90 days, have a minimal age of one day, and not be allowed to use the previous 15 passwords as a new password. Non administrative passwords shall be a minimum of 8 characters.

f. TfL shall have a documented account lockout process such that after a set number of failed login attempts the account is locked for a standard period of time.

g. TfL will regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.

h. TfL will review all system accounts and disable any account that cannot be associated with a business process and owner.

i. TfL accounts will have an automatic expiration date associated with the account.

j. TfL will monitor account usage to determine dormant accounts that have not been used for 90 days, notifying the user or user's manager of the dormancy. After a longer period, such as 90 days, the account will be disabled.

k. TfL shall ensure when a dormant account is disabled, any files associated with that account should be encrypted and moved to a secure file server for analysis by security or management personnel.

l. TfL shall establish a process, approved by the CISO, to allow line managers and supervisors to view individual accounts.

m. TfL shall review elevated account access periodically and no less than yearly.

3.18 Data Loss Prevention

3.18.1 Definition:

The processes and tools used to track/control/prevent/correct data transmission and storage, based on data content and associated classification.

3.18.2 Requirement:

a. TfL will deploy industry approved encrypted USB and hard drives for sensitive data and portable hard drives hard drive encryption software to mobile devices and systems that hold sensitive data. Such as PGP® Whole Disk Encryption or Bitlocker, using 256-bit AES encryption as a minimum.

b. The TfL Information Security Classification Standard identifies the processes for handling TfL Restricted and TfL Confidential information.

c. TfL shall employ an automated tool on network perimeters that monitors for certain sensitive information (i.e., personally identifiable information), keywords, and other document characteristics to discover unauthorised attempts to infiltrate data across network boundaries and block such transfers while alerting information security personnel.

d. The TfL network DLP tool shall be capable of identifying unauthorised data leaving the organisation, by all media – e.g. network processes like email or removable media. In addition the DLP solution should monitor and control the flow of data within the network. Any anomalies that exceed the normal traffic patterns shall be noted and flagged.

3.19 Incident management

3.19.1 Definition:

The process and tools to make sure an organisation has a properly tested plan with appropriate trained resources for dealing with any adverse events or threats of adverse events.

3.19.2 Requirement:

a. TfL will ensure that there are written incident response procedures that include a definition of personnel roles for handling incidents. The procedures shall define the phases of incident handling.

b. TfL will assign job titles and duties for handling computer and network incidents to specific individuals.

c. TfL will define management personnel who will support the incident handling process by acting in key decision-making roles.

d. TfL shall devise organisation-wide standards for the time required for system administrators and other personnel to report unusual events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification.

e. TfL shall assemble and maintain information on third-party contact information to be used to report a security incident.

f. TfL shall publish information for all personnel, including employees and contractors, regarding reporting computer anomalies and incidents to the incident handling team.

g. TfL shall conduct periodic security incident scenario sessions for personnel associated with the incident handling team.

3.20 Lockdown Network Control

3.20.1 Definition:

The process and tools used to build, update, validate and restrict (when necessary) a network infrastructure that can properly withstand attacks from advanced threats.

3.20.2 Requirement:

a. TfL shall design the network using a minimum of three-tier architecture (DMZ, middleware, and private network). Any system accessible from the Internet shall be on the DMZ, DMZ systems shall not contain sensitive data.

b. TfL shall segment the enterprise network into multiple, separate trust zones to provide more granular control of system access and additional intranet boundary defences.

3.21 Penetration Testing

3.21.1 Definition:

The process and tools used to simulate attacks against a network device, to validate the overall security of an organisation.

3.21.2 Requirement:

a. TfL will conduct monthly external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully.

b. TfL penetration testing shall occur from outside the network perimeter (i.e., the Internet or wireless frequencies around an organisation) as well as from within its boundaries (i.e., on the internal network) to simulate both outsider and insider attacks.

c. TfL shall create an auditable process for creating and executing penetration testing.

d. TfL with the support of the information owners will perform periodic red team exercises to test organisational readiness to identify and stop attacks or to respond quickly and effectively.

e. TfL shall use a dedicated account for authenticated penetration testing. The account should be tied to specific machines at specific IP addresses, only be used by authorised employees and not be used for any other activity.

f. TfL shall ensure that systemic problems discovered in penetration tests and red team exercises are fully tracked and mitigated.

g. TfL shall ensure a penetration test on all new systems before go live.

3.22 Compliance Monitoring

3.22.1 Definition:

The process and tools used to monitor compliance of the TfL critical controls.

3.22.2 Requirement:

a. TfL shall identify the critical systems on the network.

b. TfL shall run automated compliance scanning tools against network information security controls/policies.

c. The timing of the compliance checking will depend on the nature of the system. No system shall go longer than a year without compliance checking.

3.23 Exception Control

3.23.1 Definition:

The processes and tools used to track/control/prevent/correct/minimise the use of system and application exceptions.

3.23.2 Requirement:

a. TfL shall review all system and application exceptions, and upon discovery, disable any exception that cannot be associated with a business process owner and/or an active TfL account.

b. TfL exception control shall have an automatic expiration date associated with the exception.

c. TfL will automatically create an exception report on a monthly basis, by business owner. The business owner shall review and acknowledge responsibility for exceptions.

3.24 Physical Security

3.24.1 Definition:

The processes and tools used to identify/track/control/prevent/correct physical secure access to information and systems according to the formal determination of which persons, computers, and applications have a need and right to access based on an approved need.

3.24.2 Requirement:

a. TfL requires an appropriate level of physical security to protect information assets from any unauthorised use.

b. TfL environments which contain sensitive information shall be restricted and not allocated to staff members by default as part of a standard building access profile.

c. TfL server rooms, data centres and control centres shall log all ingress and egress activities.

d. TfL operates a clear desk and screen policy helps reduce the chance that information could be inappropriately disclosed to other staff or visitors and also reduces the chance of disclosures happening after-hours caused by cleaners or break-ins.

e. TfL printers will use identity card roles to release print material.

3.25 Encryption

3.25.1 Definition:

The process for protecting data using encryption.

3.25.2 Requirement:

a. TfL data in transit and data at rest shall be encrypted as per the Information Classification Protection Requirements.

b. Encryption of TfL data shall use 256-bit AES encryption, as a minimum.

c. Provide HMG approved crypto storage

d. Identify crypto custodian

3.26 Policy Maintenance

3.26.1 Definition:

The process of creating, validating and maintaining an information security policy, instruction or principle, that maps to a control in this framework.

3.26.2 Requirement:

a. TfL shall ensure that there are written policy and/or procedures that correspond to the controls framework.

b. TfL shall have a communications plan for policy release.

c. TfL shall perform a yearly review of all Information Security Policies, principles and standards.

d. TfL shall ensure that all policies are traceable to a requirement in the controls framework.

3.27 Information Disposal

3.27.1 Definition:

The process to ensure information being destroyed is non-recoverable, using methods commensurate to the sensitivity of information.

3.27.2 Requirement:

a. TfL shall ensure the destruction of information ensures the confidentiality and TfL complies with legislative and contractual requirements such as the Data Protection Act 1998, PCI DSS and any classification requirements.

b. TfL shall protects information system media until the media are destroyed or sanitised using approved equipment, techniques, and procedures

c. TfL shall employ sanitisation mechanisms with the strength and integrity commensurate with the security category or classification of the information.

d. TfL shall provide a secure means to dispose of paper products that contain sensitive information.

e. TfL shall ensure any exceptions to this policy are formally documented, and signed off by the CISO.

3.28 Third Party Computing

3.28.1 Definition:

The process for storing, processing and/or accessing of data on a production ready Third party based service.

3.28.2 Requirement:

a. The TfL data owner shall approve the hosting of TfL information on a third party system.

b. Third party services shall be hosted on a production ready non experimental third party system.

c. Data that will be handled by a third party provider shall first consider the level of classification of the data.

d. If data to be handled by the Third party provider has not been formerly classified the TfL data owner shall classify the data.

e. Data ownership shall remain with TfL.

f. The third party provider shall make certain compliance with the UK Data Protection Act. Any TfL confidential information shall not be held outside the EU.

g. The Third party provider shall have an incident response process in place, including a documented approach to security breaches that addresses identification, response, recovery and review. The Third party provider shall inform TfL immediately if an information security incident affecting TfL information or information services occurs.

h. TfL and the Third party provider shall agree that TfL has full access to TfL data at any time. TfL shall have an agreed upon mechanism to export data during termination services; and an audit mechanism to make certain data is purged including sanitisation of obsolete hardware and all Meta data.

i. The long term viability of the Third party provider shall include a documented agreement on what would happen to TfL service or data if the provider is acquired or goes into insolvency.

j. The third party shall maintain an access log of all TfL data.

k. The third party shall abide by the ISCF.

3.29 Information Asset Register

3.29.1 Definition:

The process for identifying, classifying and assigning owners to the TfL information asset register.

3.29.2 Requirement:

a. TfL shall create and maintain an information asset register.

b. TfL shall appoint and train Information Asset Owners.

c. The register shall identify information type, e.g. Strategy papers, the classification and the associated risk score

d. TfL shall update the asset register annually.

4 Supporting Information

a. Abbreviations

The following abbreviations are created:

Abbreviation	Definition
AD	Active Directory
AES	Advanced Encryption Standard
CISO	Chief Information Security Officer
DMZ	Demilitarised Zone
EU	European Union
HMG	Her Majesty's Government
IPS	Intrusion Protection System
ISCF	Information Security Controls Framework
PGP	Pretty Good Privacy
SQL	Structured Query Language
TCP	Transfer Controls Protocol
USB	Universal Serial Bus
VPN	Virtual Private Network
WPA	Wi-Fi Protected Access

b. Definitions

The following definitions are created:

Term	Definition

5 References

Centre for Internet Security (CIS);

International Organisation for Standardisation (ISO);

SysAdmin Audit Network Security (SANS) Institute;

National Institute of Standards Technology (NIST).