# PICTS Contract

# Schedule 3

# PROVIDER’s SOLUTION

**Document Info**

**Version #:** 1.0

**Date:** 15 December 2016

**Revision History**

| Version | Date | Details of Changes | Author |
|---|---|---|---|
| 1.7 (SSG) | 13/11/16 | PM Draft circulated for review | Sopra Steria |
| 1.8 (SSG) | 14/11/16 | SA Mark-up | Sopra Steria |
| 0.1 | 15/11/16 | PM mark-up | Sopra Steria |
| 0.2 | 17/11/16 | Joint mark-up of Serv Mgt | Sopra Steria & MoJ |
| 0.3 | 23/11/16 | Tidy up and inclusion of comments on DR | Sopra Steria |
| 0.7 | 12/12/2016 | Joint workshop | Sopra Steria & MoJ |
| 0.8 | 14/12/2016 | Updates post workshop | Sopra Steria |
| 0.9 | 15/12/2016 | Baselined | Sopra Steria & MoJ |
| 1.0 | 15/12/2016 | Final version for completion | Sharpe Pritchard |

## SCHEDULE 3 – PROVIDER'S SOLUTION


1 INTRODUCTION ..... 3
2 SOLUTION OVERVIEW ..... 4
3 END USER COMPUTING ..... 5
4 APPLICATION SERVICES ..... 7
5 DATA SERVICES ..... 8
6 MANAGEMENT INFRASTRUCTURE ..... 10
7 DISASTER RECOVERY ..... 11
8 GATEWAY, NETWORK AND SECURITY ..... 11
9 SERVICE MANAGEMENT TOOLS ..... 12
10 DATA CENTRE SERVICES ..... 13
11 VISOR SERVICE ..... 15
12 NDELIUS SERVICE ..... 15
13 BLACKBERRY SERVICES ..... 15
14 PROJECT SERVICES ..... 17
15 OTHER SERVICES ..... 17
16 SERVICE DESK ..... 17
17 INCIDENT MANAGEMENT ..... 19
18 PROBLEM MANAGEMENT ..... 19
19 REQUEST MANAGEMENT ..... 20
20 CHANGE MANAGEMENT AND RELEASE MANAGEMENT ..... 20
21 MONITORING AND EVENT MANAGEMENT ..... 21
22 CAPACITY MANAGEMENT ..... 22
23 AVAILABILITY MANAGEMENT ..... 22
24 SECURITY MANAGEMENT ..... 23
25 CONFIGURATION MANAGEMENT ..... 23
26 SERVICE REPORTING ..... 23
27 DISPOSAL SERVICE ..... 24
28 ISO STANDARDS ..... 24
A. ANNEX A – HEATMAP ..... 26
B. ANNEX B – VOLUMETRICS ..... 28
C. ANNEX C – KEY PERSONNEL ..... 29
D. ANNEX D – DISASTER RECOVERY ..... 31
E. ANNEX E – DESCRIPTION OF OPERATIONAL RISK ..... 36
F. ANNEX F - SOFTWARE AND SUPPORT ..... 37

# 1 INTRODUCTION

1.1 Following this introductory section, this Schedule 3 (PROVIDER'S Solution) comprises the following sections:

(a) Main Body - PROVIDER Services – Technology, People and Process

(b) Annex A – Heatmap

(c) Annex B – Volumetrics

(d) Annex C – Key Personnel list

(e) Annex D – Disaster Recovery

(f) Annex E – Description of Operational Risk

(g) Annex F - Software and Support

(h) Annex G – Not Used

(i) Annex H – ViSOR services

1.2 This Schedule 3 (PROVIDER'S Solution) describes:

(a) the Services that the PROVIDER will provide in accordance with the terms of this Agreement

**PROVIDER Services – Technology, People and Process**

## 2 SOLUTION OVERVIEW

2.1 The PROVIDER will supply the following Services:

- End User Computing (EUC)
- Application Services
- Data Services
- Central Infrastructure
- Gateway, Network and Security
- Service Management Tools
- Data Centre Services
- ViSOR Service
- nDelius Service (NB. May have transitioned at the Commencement Date)
- Blackberry Service
- Project Services
- Other services

2.2 The Services as at the Commencement Date are described in this Schedule 3 and summarised in Figure 1.

2.3 Annex A of this Schedule provides a Heatmap summarising the service and security risks associated with the current Platform, as at the Commencement Date.

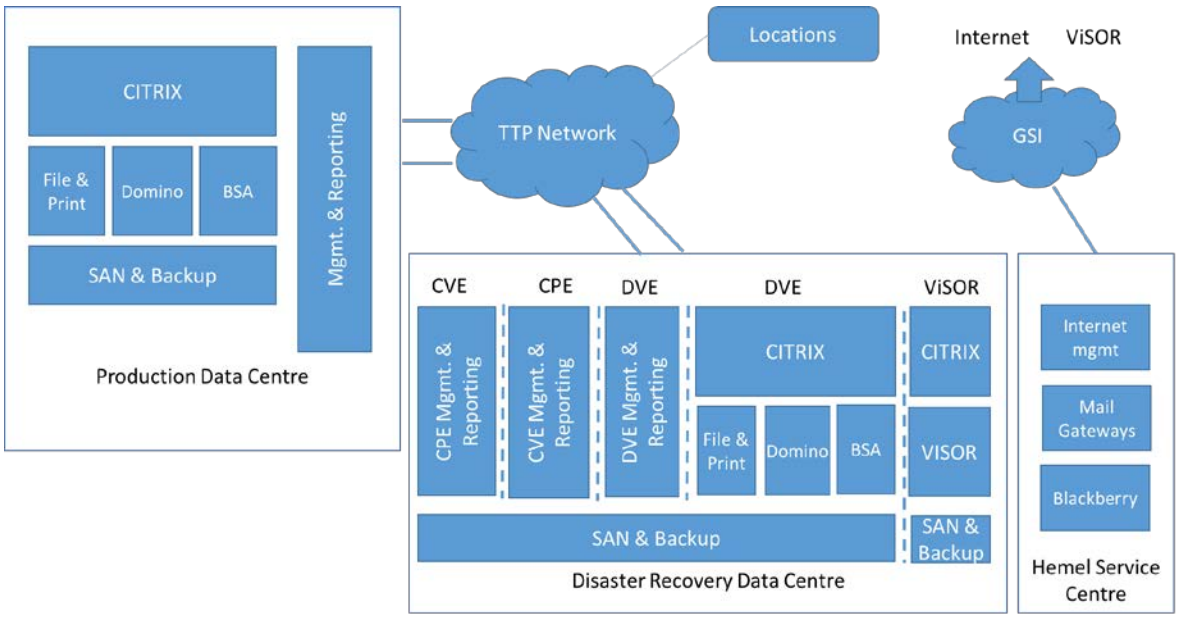


Figure 1 – PICTS Services

2.4 Schedule 16 describes any Technology Refresh activity that may update or change the Services provided by the PROVIDER.

## 3 END USER COMPUTING

3.1 The PROVIDER will provide Workstations and End User Services to enable Users to access Application Services, Data Services and the Infrastructure. Workstations consist of:

3.1.1 Thin-client devices – The majority of End Users use Thin-clients. . A Thin-client consists of the Thin-client device, a monitor, a keyboard and mouse. A Thin-client device enables access to the Services via Citrix. The number of Thin-clients to be supported at the Commencement Date is stated in Annex B.

3.1.2 Laptops – End Users with mobility requirements are provided with Laptops. The number of Laptops to be provided by the PROVIDER is stated in Annex B. End Users with Laptops can access Citrix and Thick-client Services. The number of Laptops to be supported at the Commencement Date is stated in Annex B.

3.1.3 Desktops – A number of desk based End Users have Desktops. These provide access to Citrix and Thick-client Services. The number of Desktop to be supported at the Commencement Date is stated in Annex B.

3.1.4 AT Laptops – A specially built device for users with Assistive Technology requirements. These devices have Assistive Technology Tools deployed to aid the use of IT for Users with a disability (AT Users). The number of AT Laptops to be supported at the Commencement Date is stated in Annex B.

3.2 End User Services consist of the following:

3.2.1 a Citrix Server solution that will provide access to applications for End Users from Thin-client devices, Desktops and Laptops. The number of Citrix Servers to be provided by the PROVIDER is stated in Annex B. The Citrix solution contains:

(a) a number of Citrix silos:

i Core NPS (CORE03) - NPS Users core applications

ii Core CRC (CORE01) - Core applications for CRC Users and CRC Exception Users

iii Flash Silo (NONCORE12) - NPS Users Flash enabled applications

iv Shared Service Silo (NONCORE13) – Used by NPS Users to access Phoenix application (time recording)

(b) Data Collectors & Management Servers:

i Citrix data collectors used by the PROVIDER to manage the farm, not accessed by Users

ii Used by the PROVIDER and AUTHORITY IT staff to run management consoles

3.2.2 Workstation Applications – the following Workstation Applications will be accessible from the Workstation:

| Applications | Base Build | ICT Admin | AT Users | Laptops |
|---|---|---|---|---|
| Adobe Reader 9.5.5 | Yes | Yes | Yes | Yes |
| Office 2003 with Welsh Language | Yes | Yes | Yes | Yes |
| Office 2007 Compatibility Pack | Yes | Yes | Yes | Yes |
| WinZip 11.1 | Yes | Yes | Yes | Yes |
| Lumension Client 4.2 | Yes | Yes | Yes | Yes |
| Mozilla Firefox 31.1.1esr | Yes | Yes | - | Yes |

| | | | | |
|---|---|---|---|---|
| McAfee VirusScan 8.8P2 | Yes | Yes | Yes | Yes |
| Shadow Copy Client | Yes | Yes | Yes | Yes |
| ICA Client 12.1 | Yes | Yes | Yes | Yes |
| EPIC Icon | Yes | Yes | Yes | Yes |
| Ndelius Live | Yes | | | |
| Ndelius Training | Yes | | | |
| | | | | |
| Lotus Notes Basic Client | - | Yes | Yes | Yes |
| Lotus Notes Admin Clients | - | Yes | - | - |
| OMNI ICT Admin MMC Plugins | - | Yes | - | - |
| Offer Remote Assistance desktop shortcut | - | Yes | - | - |
| Custom CMD Utilities | - | Yes | - | - |
| AT ToolBox | - | - | Yes | - |
| Dragon Naturally Speaking | - | - | Yes | - |
| Adobe Flash player 11.9 | - | - | Yes | - |
| Java Runtime Environment | - | - | Yes | - |
| Java Archive files | - | - | Yes | - |
| AT Read Write | - | - | Yes | - |
| Mozilla Firefox 17.11 (Only for AT Users) | - | - | Yes | - |
| Secure Office Client | - | - | - | Yes |
| Juniper NetConnect Client 7R4 | - | - | - | Yes |
| Gemalto dot net driver (Smart Card driver) | - | - | - | Yes |

Table 1 – Workstation build information

3.2.3 End Point Protection which provides a level of protection to the Workstations:

(a) Lumension – prevents the use of unauthorised peripherals, such as USB devices.

(b) Smart Cards – Smart Cards provide additional security for User authentication by requiring the End User to know a passcode and have a physical card to corroborate their authentication.

(c) Secure Office – Secure Office provides encryption of Laptops and Desktops to prevent loss of data where Laptops or Desktops are lost or stolen.

3.2.4 AT Tools will be provided as part of the build for AT Users. These tools are shown in table 1 above, and include: AT Toolbox, Dragon Naturally Speaking, AT Read Write

3.2.5 Print Management – End Users are able to print from Workstations to authorised Print Devices. The PROVIDER will support printing on Workstations and the associated print servers and print queues. The PROVIDER will not provide any support or other services for Print Devices. The AUTHORITY's Print Tower Supplier (currently Xerox) will provide support of the Print Devices.

3.2.6 Scan to folder – The PROVIDER will provide End Users with the ability to scan documents to a data folder from a Print Device. Legacy Print Devices will be able to scan to Windows File services from which End Users can retrieve their scanned documents. Print Devices will be able to scan to a Windows File server which then copies files to NPS file storage (NetApps).

## 4 APPLICATION SERVICES

4.1 The PROVIDER will provide Application Services for End Users. Applications Services consist of Business Support Applications (BSA), Domino Applications, Libra and Email/Calendaring.

4.1.1 Business Support Applications will be hosted as detailed in the following paragraphs;

4.1.2 The PROVIDER will supply a managed infrastructure in accordance with the BSA Service Definition Document (Ref. SM_SM_SDD_14_424_OMNI NPS Business Support Application SDD). The AUTHORITY will manage the installation, management and support of those Applications hosted on the BSA platform.

4.1.3 The BSA platform is accessible by Citrix only and access is limited to Users in the NPS.

4.1.4 The following BSAs will be hosted on the BSA platform:

(a) Nimbus

(b) Workload Management Tool

(c) RSR

(d) Victims

4.2 The PROVIDER will provide a Domino Application hosting environment on the Lotus Domino Platform. The AUTHORITY will manage the development, management and support of those Applications on the Domino Applications hosting environment

4.2.1 Mail databases and transaction logs will be held on Central File Storage

4.3 Libra is used to access information concerning Magistrate's Courts including a case management system. Libra will be able to be accessed from the Internet Browsers on the Workstation.

4.4 Access to the XHBIT Daily Court Status application, which provides information in regards to court hearing schedules and notes.

4.5 Email/Calendaring – the PROVIDER will provide End Users with the ability to access email and calendaring from a Lotus Notes Domino solution.

4.5.1 The email solution will enable other Criminal Justice organisations to exchange email with the AUTHORITY, and provide external email capability through the Government Secure Intranet (GSi).

4.5.2 The PROVIDER will provide a spam filtering service for email received from the Internet. The PROVIDER will maintain the spam filtering rules to minimise the amount of unwanted email received by Users.

4.6 The PROVIDER will provide Internet Access to the Users via GSi via the Workstation.

4.6.1 The PROVIDER will implement content filtering services, as a defence against User access to inappropriate content, by allowing the AUTHORITY to define Internet filtering groups, which will then be applied by the PROVIDER to the Users from within the Active Directory Service, to meet the AUTHORITY's requirement for control of access to Internet sites.

4.6.2 The PROVIDER will provide web filtering report services, whereby the PROVIDER will produce custom and predefined reports of historical Internet and Application

access by Users suitable for use by the AUTHORITY to identify contraventions of its Internet usage policies and to support the processes of Security.

## 5 DATA SERVICES

5.1 Data Services consist of File services and Backup services. The Data Services solution is summarised in Figure 2.

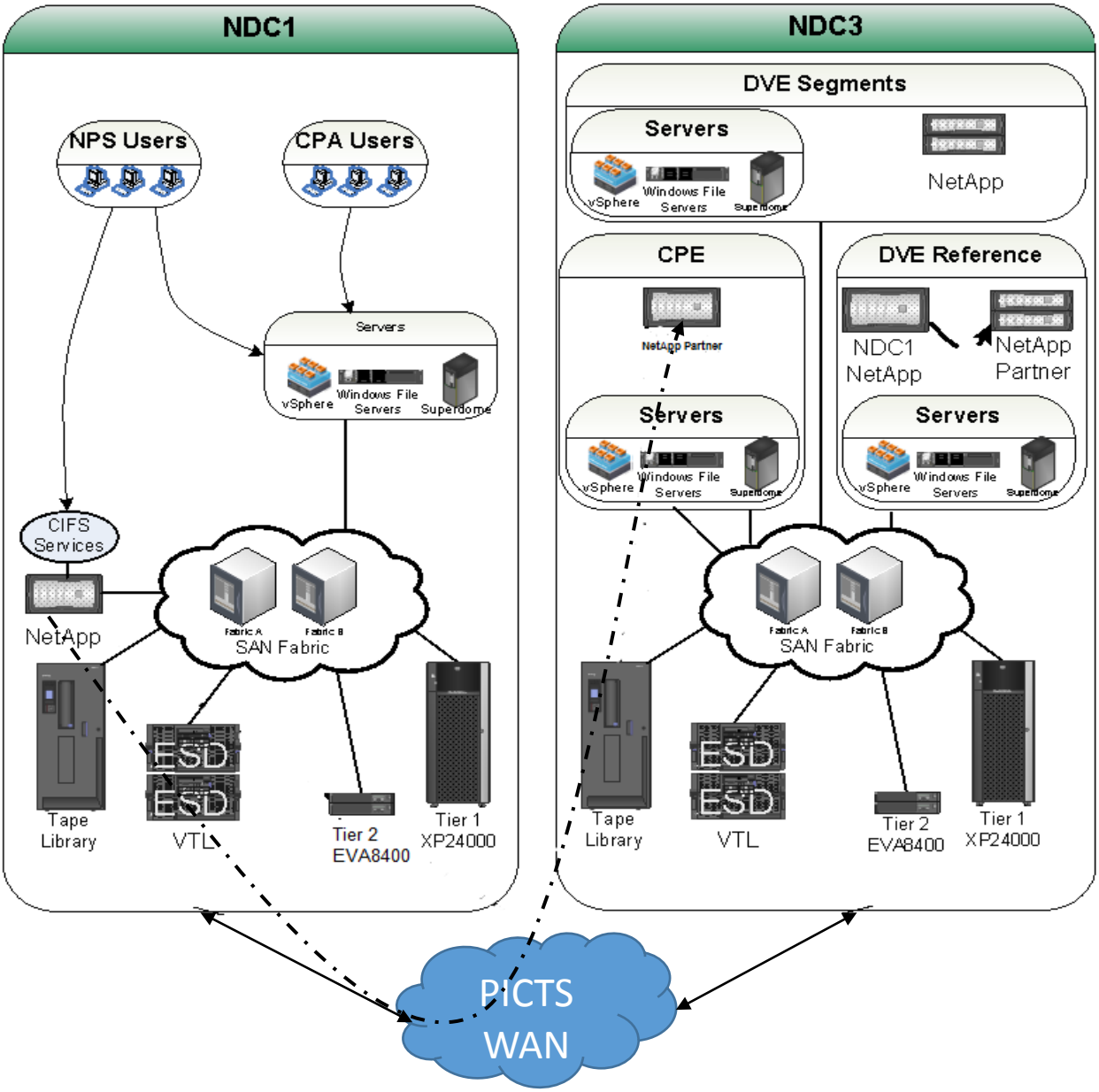


**Figure 2– Data Services solution overview**

5.2 File services

5.2.1 The components of the Storage Services infrastructure comprise the following infrastructure, the storage solution is summarised in Figure 2:

(a) HP XP24000 and EVA8400 storage system providing Tier 1 and Tier 2 storage services, including CRC User and shared data

(b) NetaApp file service for NPS User and shared data.

(c) McAfee VirusScan Enterprise for Storage (VSES) n NDC1 and NDC3

(d) DEBS file share in NDC3 for enabling DEBS users to access reports produced via nDelius Reporting

5.2.2 The Tier 1 and 2 storage solution is configured as follows:

(a) The Production Data Centre has an HP XP24000 storage array connected to a SAN providing both Tier 1 and Tier 2 storage.

(b) Tier 1 storage provisions from internal XP24000 capacity.

(c) Tier 2 storage provisions from an externally attached, HP EVA8400 storage array.

(d) The XP24000 provides at least 36 TB of usable Tier 1 and 40 TB of Tier 2 storage.

(e) The XP24000 provides data volumes to application and infrastructure Servers.

(f) HP EVA8400 storage arrays are configured to provide the capability to present storage as external storage to the XP24000 and directly to servers where required.

5.2.3 The NetApp storage solution is configured as follows:

(a) Two NetApp controllers FAS6620A deployed in both National Data Centres.

(b) One FAS6220A and two FAS3250AE controllers hosted in DVE to support Development and Testing.

(c) All NetApp controllers run the Data ONTAP operating system in 7-mode. Windows file shares are available using the licensed CIFS protocol; the only protocol configured on the controllers.

(d) The existing AD environment continues to control access to files and folders.

(e) The NetApp file data is backed up locally using NetApp snapshots which is as replicated over the network to the controllers in the Disaster Recovery Data Centre for use in a Disaster.

(f) The files are scanned by Anti-Virus, monitored with auditing and growth restricted by the use of quotas.

(g) The controllers have been configured with at least 50TB of storage.

(h) All controllers, use the vFiler feature for provision of file services. Management functions utilising OCUM, OCSM.

(i) Config Advisor is deployed into the CPE environment.

5.2.4 The Data Recovery Data Centre has infrastructure to support the DVE, CPE, CVE or provide DR facilities for the failure of the Production NDC. The CVE utilises HP StorageWorks 8/80 switches to provide access to an EVA8400 storage

5.3 Backup Services:

5.3.1 A Virtual Tape Library (VTL) solution, which will be deployed in the Production and Disaster Recovery Data Centres based on IBM technology. Production data will

be backed up by the VTL within the Production Data Centre and then replicated to the Disaster Recovery Data Centre.

5.3.2 In addition data stored within the NetApp is backed up and restored via the NetApp replication service.

5.3.3 The retention policy for data is as described in the NDC Policy Spreadsheet (OSD-1108BI)

5.3.4 The standard backup retention policy may be changed for specific backups if any one of the following scenarios applies:

(a) The data is temporary and does not require to be backed up.

(b) Where backups are only required for Disaster Recovery purposes in which case either:

i Only the last successful backup is required; or

ii The server can be rebuilt from the package tool (e.g. Radia) and hence no backups are required

(c) Where Applications provide facilities to recover old data, in which case the backup retention policy will be agreed with the AUTHORITY on a case by case basis.

(d) Where restore from backed up data is not beneficial after a given period of time, in which case the backup retention policy will be agreed with the AUTHORITY on a case by case basis. (eg. an application database cannot be recovered to a point several days old as it will require the business to re-key significant quantities of data).

5.3.5 Changes from the standard backup policy will be agreed through approval by the AUTHORITY of changes to the backup design documentation and, if necessary, will be formally captured through the Change Control Procedures.

5.3.6 The PROVIDER will enable Users to restore previous versions of files held in the Private and Shared File Storage areas by means of an volume shadow copy service available on the Workstations. This service will enable users to view, copy or restore previous versions of files. Eight copies of data are held (5 daily and 3 weekly) with snapshots of the NDC file cluster taken daily from Tuesday to Saturday. Retention period for shadow copies will be as follows:

(a) Saturday snapshots will be kept for 28 days

(b) Tuesday to Friday snapshots will be kept for 7 days

5.3.7 The PROVIDER shall provide a file restoration service for files held on virtual tape backup service. This service will restore files within 24 hours of the request. The PROVIDER shall additionally offer a Service that will restore files within 4 hours of the request via the Catalogue.

## 6 MANAGEMENT INFRASTRUCTURE

6.1 The PROVIDER will provide a Management Infrastructure that supports other services. The Management Infrastructure will include the following:

6.1.1 Active Directory Service, which is used to provide Role Based Access Control (RBAC) to centrally manage and maintain User access and permissions in line with AUTHORITY access control policies. Specifically Active Directory Service is used for:

(a) authentication of Users

(b) authorisation of Users to ensure that Users only access systems that they are authorised to access

(c) a central User repository

(d) management of group policies

(e) logging of logon activities by the Users

6.1.2 The following tools, which are used to manage and control the deployment of Software:

(a) Build management software, including Radia and KN3 build manager – deploys and controls the software builds of the majority of the Servers, Laptops and Desktops except where a manual build has been created. The Build Management Software will be used to patch Servers, Laptops and Desktops.

(b) Thin-client device manager – the PROVIDER will provide a Thin-client device manager to manage the deployment of firmware to Thin-clients

6.1.3 A VPN solution that enables authorised Users to initiate a secure SSL/TLS connection from their Workstation over the Internet to the PICTS Network.

6.1.4 Anti-Virus will be provided by the following two anti-virus products:

(a) McAfee – manages anti-virus policies using a central server with an agent deployed to individual Servers, Laptops and Desktops. McAfee is for Windows based systems.

(b) Sophos – manages anti-virus for Unix or Linux based system. Sophos is used as part of the MIMESweeper solution to monitor email messages for viruses

6.1.5 Certificate Management

(a) Certificate Authority – the PROVIDER will provide the Certificate Authority, which creates, issues and stores certificates for Servers, Desktops and Laptops. The OMNI CA is the master certificate store. The certificates provide a mechanism to validate the identity of a specific device.

(b) Secure Office Certificate Authority – the PROVIDER will provide the Secure Office CA which creates, issues and stores certificates for Smart Cards.

## 7 DISASTER RECOVERY

7.1 The provisions for Disaster Recovery are described in Annex D of this Schedule 3.

## 8 GATEWAY, NETWORK AND SECURITY

8.1 The PROVIDER will provide a Gateway, network services and Security services. These will consist of:

8.1.1 NDC LAN Infrastructure – the PROVIDER will provide the switches and cabling contained within the National Data Centres.

8.1.2 HSC LAN Infrastructure – the PROVIDER will provide support of switches and firewalls as noted within the CMDB.

8.1.3 A DHCP service that will be utilised by the LAN to provide IP addresses for infrastructure devices in the National Data Centres and other Locations. This excludes the voice network.

8.1.4 LAN Management Software (TACACS+) – a mechanism for authenticating to network devices using Cisco ACS. Cisco ACS is an access control policy platform that provides TACACS+ and Radius authentication, authorisation and accounting services to managed network devices.

8.1.5 GSI Gateway, which enables connectivity from within the PICTS Network to the GSI and public Internet. The GSI connection will be provided and managed by the AUTHORITY. The GSI Gateway will provide Network connectivity to:

(a) Mail

(b) Blackberry

(c) ViSOR

(d) LIBRA

(e) XHBIT

(f) PSN

(g) Internet

(h) PSN / GSI services

8.1.6 The GSI gateway network contains two DMZ network segments that act as a security perimeter between the estate and the GSI/Internet.

8.1.7 There will be no Disaster Recovery solution for the GSI Gateway

8.1.8 Firewalls – the PROVIDER will support the Firewalls listed in Annex B of this Schedule 3.

8.1.9 Intelligent Web Gateway – the PROVIDER will provide an Intelligent Web Gateway solution using M86 Secure Web Gateway solution that automatically scans web page content for viruses and malware.

8.1.10 MIMESweeper – the PROVIDER will provide MIMESweeper using Sophos to check email content for viruses and malware within Lotus Notes Domino and Blackberry.

8.1.11 Internet Security and Acceleration Server (ISA) – the PROVIDER will provide ISA, which acts as an upstream proxy and permits web traffic authorised by the Intelligent Web Gateway and both incoming and outgoing MIMESweeper traffic to pass through to the Internet.

## 9 SERVICE MANAGEMENT TOOLS

9.1 The PROVIDER will provide the following tools to support the management of the Services:

9.1.1 A central alert processing and management platform that receives events from all managed tools and is able to pass them to the Service Desk tool based on the rules configured within the OpenView monitoring toolset.

9.1.2 HP Network Node Manager - The PROVIDER will provide an HP NNM instance to execute the following network management activities:

(a) Central trap handling facility

(b) Active monitoring

9.1.3 The following sources will provide alerts to NNM within the estate:

(a) Any Simple Network Management Protocol (SNMP) enabled device on the network with the NNM server configured as the trap destination

(b) Citrix Resource Manager (CRM) which acts as a central repository for all Citrix faults and forwards them as SNMP traps to NNM

(c) SAN and tape storage infrastructure

(d) HP SIM agents

(e) iLo management cards

9.1.4 HP Business Activity Centre – the PROVIDER will provide HP BAC to support the Service Level reporting. This enables Service availability and performance of certain Applications to be monitored and measured by performing synthetic user transactions or probes against the relevant Applications.

9.1.5 Enhanced LAN monitoring solution based on the Solarwinds toolset, to monitor and alert on the performance of the Data Centre LAN.

9.1.6 The PROVIDER will provide a system logging infrastructure (SLS) that will maintain event data for a rolling period of 12 Months in the following areas:

(a) Archiving of Windows-based system event logs

(b) Archiving of the Domino Mail server message tracking logs

(c) Archiving of messages generated from syslog clients

(d) Archiving of Windows log files, such as DHCP and IIS

(e) Archiving of NetApp vfiler system and user event data

9.1.7 HP Service Desk – the PROVIDER will provide a dedicated Service Desk tool that is used to support ITIL functions. The Service Desk uses HP Service Manager as its underlying software platform.

## 10 DATA CENTRE SERVICES

10.1 The PROVIDER will provide Data Centre Services to accommodate Server Hardware, Network and storage devices. The Data Centre Services will consist of:

10.1.1 NDC1 – NDC1 will accommodate the Production Data Centre, providing sufficient rack space, power and cooling for the hardware and devices hosted within it. Further volumetrics concerning NDC1 can be found in Annex A of this Schedule 3.

10.1.2 NDC3 – NDC3 accommodates DVE and DVE REF, the Disaster Recovery environment and monitoring and management servers, providing sufficient rack space, power and cooling for the hardware and devices hosted within it. This environment is summarised in Figure 3.

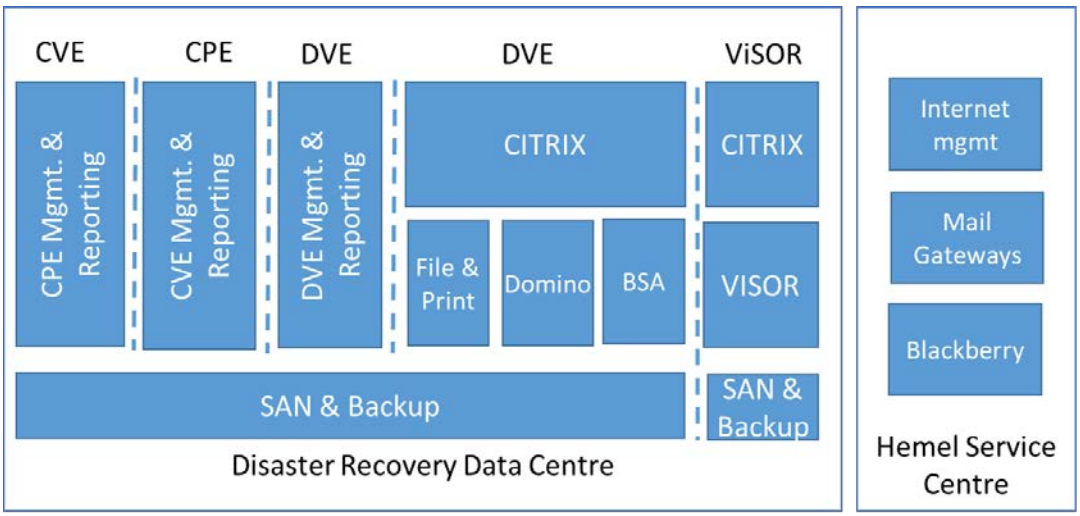


**Figure 3 – NDC Summary**

10.1.3 Details of the environments to be provided are as follows:

(a) A Development Validation Environment (DVE) that will provide infrastructure to enable effective integration of the modified components to take place. This environment will be established and managed by the PROVIDER's environments team under the control of the Change Management process. The DVE environment will be split into a number of Segments. A Segment is a subset of the System located in DVE that enables changes to be developed and tested in isolation without affecting the live environment. Each Segment will be structured slightly differently to enable different Changes to be tested. Testing in multiple Segments can occur concurrently. A number of Segments within this environment will have limited/restricted connectivity to the Internet.

(b) A Development Validation Reference Environment (DVE REF) which will provide infrastructure as close to live infrastructure as practical to enable final verification tests to occur, including enabling acceptance testing of the modified components to take place. This will include resilient components to enable tests of redundancy modes and component failover and sufficient infrastructure to enable a degree of scaled performance testing. This environment is established and controlled with packages deployed into the environment by the PROVIDER's Support Organisation under the Change Management process. This environment will have limited anonymised user data provided by the AUTHORITY. This environment will have restricted connectivity to the AUTHORITY Strategic Partner Gateway (SPG);

(c) HSC – Hemel Service Centre – provides access to externally facing services such as the GSI. All inbound and outbound traffic out of the PICTS environment goes through the HSC environment.

(d) Computer Suite 6 – provides additional Data Centre capacity to the Disaster Recovery Centre and is managed in-line with the Disaster Recovery Data Centre.

(e) Critical Production Environment (CPE) - provides core management services across PICTS. It includes build management services, backup management services and anti-virus management services.

(f) Critical Validation Environment (CVE) - provides a small test Segment that would remain available in the event of a disaster to enable the PROVIDER with the ability to test security patches prior to deployment.

10.1.4 The PROVIDER will provide and maintain a Segment Plan that will show what Segments are in use for what purpose. Segments will be booked out via the Segment Plan.

## 11 VISOR SERVICE

11.1 The ViSOR service will be provided as described in Annex H of this Schedule 3.

## 12 NDELIUS SERVICE

12.1 The PROVIDER has been providing an infrastructure support service in support of the nDelius Application. It is anticipated that the nDelius Application will be migrated to a Replacement Provider during 2016, but should this not prove to be the case then the PROVIDER will continue to provide the infrastructure support service until such time as the migration is achieved. This infrastructure support service is described in the OMNI Service nDelius Handbook.

## 13 BLACKBERRY SERVICES

13.1 The PROVIDER will provide a Blackberry service to End Users. The Blackberry service will consist of:

13.1.1 Blackberry Enterprise platform – this consists of a number of Servers, and a backup solution. These are configured to enable a Blackberry service for Blackberry Users. The Blackberry Enterprise platform has a replica of the Domino service enabling the Blackberry device to send and receive email and access calendaring information; and

13.1.2 Blackberry handsets – the PROVIDER provides a number of End Users with a Blackberry handset from the existing AUTHORITY owned Blackberry stock. The number of End Users with a Blackberry handset is stated in Annex B of this Schedule 3.

Figure 4 summarises the Blackberry solution.

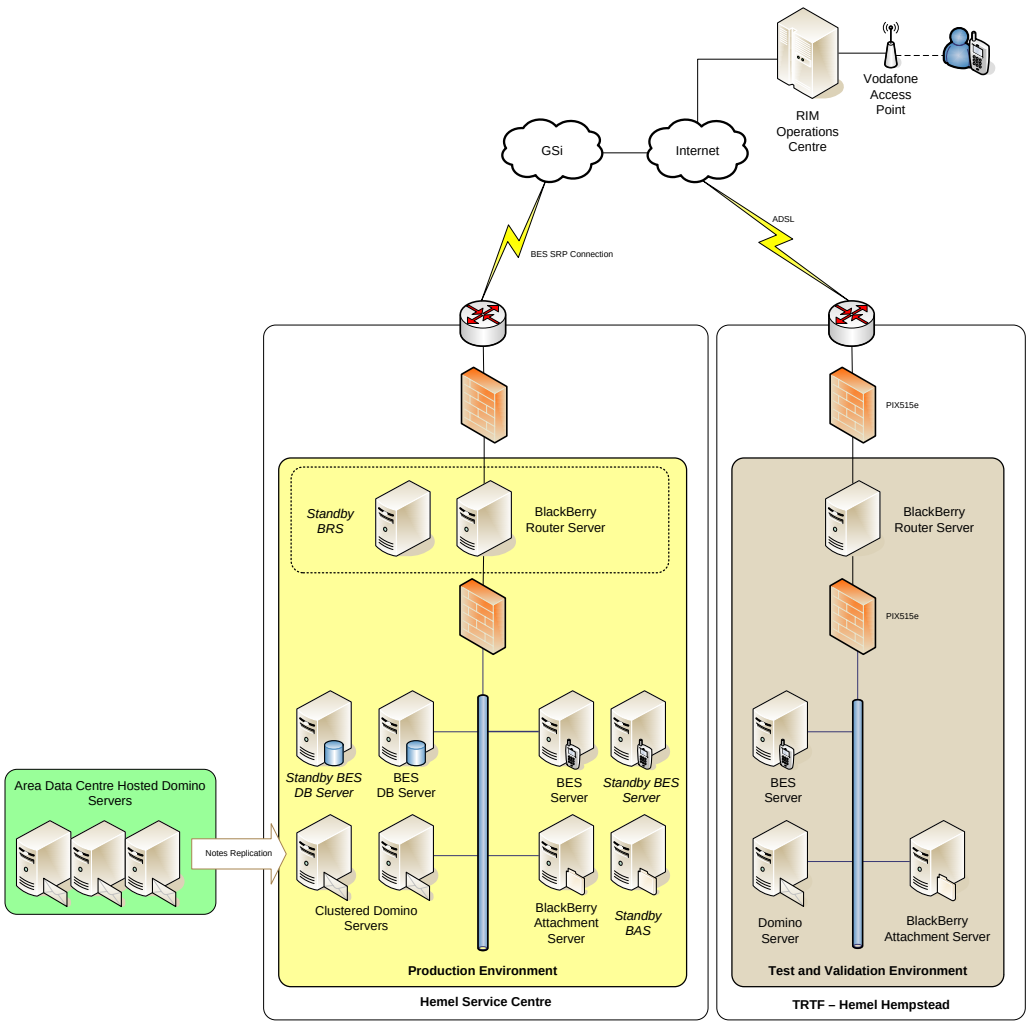


**Figure 4 – Blackberry solution overview**

13.2 The Blackberry service is suitable for the transmission of data up to Official.

13.3 The Blackberry infrastructure is designed to handle up to 1,000 connections.

13.4 The Blackberry service has not been designed to be AT compliant.

13.5 It should be noted that the PROVIDER can no longer obtain replacement Blackberry devices for the model currently in use from Vodafone and therefore replacements for lost, stolen or damaged devices cannot be provided. Where a User needs a replacement device this will be managed by the AUTHORITY via a stock of spares.

13.6 No alternative models are currently authorised for use. If the AUTHORITY requires an alternative model to be available then this will have to be requested and agreed through the Change Control Procedures.

13.7 The PROVIDER will provide a billing service for the Blackberry service, providing:

13.7.1 the monthly billing file provided by Vodafone

13.7.2 a summarised consolidated invoice (as set out in Annex A to Schedule 11)

13.7.3 a BlackBerry User summary

## 14 PROJECT SERVICES

14.1 The PROVIDER will provide project services on an ad-hoc basis when requested and agreed through the Change Control Procedures. Project services will provide the capability to deliver projects agreed with the AUTHORITY.

## 15 OTHER SERVICES

15.1 The PROVIDER will provide a number of other services detailed below ('Other Services'). Other Services will consist of:

15.2 DEBS Support Infrastructure – the following infrastructure will be used to support the Delius Exchange Bridging Solution (DEBS). The DEBS infrastructure and support service is provided by the AUTHORITY. Access to the nDelius Application from the DEBS infrastructure is provided via access infrastructure within the PICTS Infrastructure:

15.2.1 Authentication – Windows domain authentication to DEBS and network authentication to network devices in DEBS solution

15.2.2 Monitoring – SolarWinds is used for network monitoring and SNMP alerts are received by HP Service Desk

15.2.3 Management – Managed access to the DEBS infrastructure is provided by a management server

15.2.4 DEBS File Share – a file share that enables access for DEBS End Users to access reports produced via nDelius Reporting

15.2.5 Access to management services for Anti–virus

## 16 SERVICE DESK

16.1 The Service Desk will be aligned to the ITIL v3 Framework. The Service Desk will be staffed by security cleared (SC) call handlers who operate as the Single Point of Contact (SPOC) to the AUTHORITY's Call Handling Service-desk (CHS) and NPS ICT teams. The Service Desk will use the Service Management Tools to manage Incidents received and undertake Call Handling as further described in the following paragraphs. The Service Desk (situated in Warrington) will operate within Core Hours.

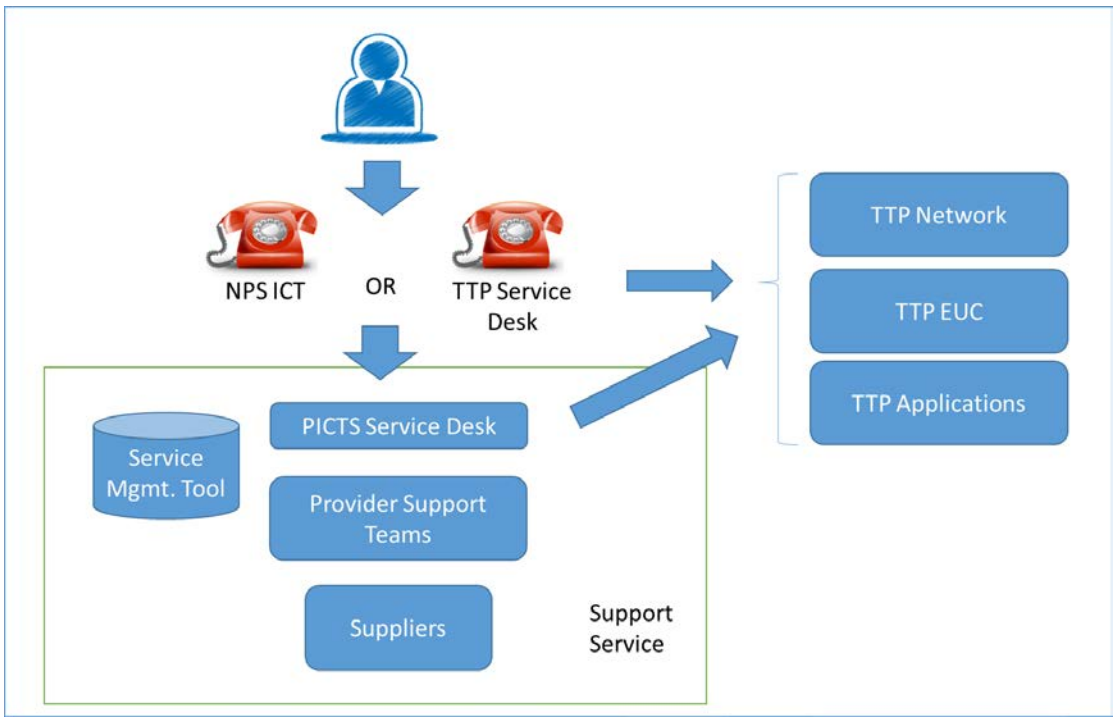


**Figure 5 – Support Model overview**

16.2 Outside of Core Hours the PROVIDER will provide a limited Non–Core Hours support service. Support services available in Non–Core Hours will only be for Severity Level 1 Incidents. The Non–Core Hours support service will be:

16.2.1 Incident logging through to managing a resolution via the on-call support and other relevant suppliers;

16.2.2 Remote Operation Centre (ROC) Monitoring – Provision of the ROC, staffed by security cleared (SC) Personnel, which will monitor alerts from the System, log Incidents appropriately and provide basic fault resolution including service restarts. The ROC team will also be responsible for deploying security patches, minimising disruption to the Services during Core Hours;

16.2.3 Handling of lost / stolen devices reported to the PROVIDER via the AUTHORITY Incident Report line.

16.3 The Service Desk, in addition to fault logging and Incident Management, will be the focal point of the ITIL support service including supporting Incidents throughout their lifecycle, whether being managed by the PROVIDER's teams or via Third Party Suppliers.

16.4 Where Incidents cannot be resolved first time by the Service Desk, they will be passed on to appropriate support service teams to resolve the Incident in line with ITIL, with the Service Desk retaining the ownership of the Incident so they can report, manage and progress the Incidents until successful resolution.

16.5 Where onsite attendance is required, the Service Desk will forward the request to the appropriate support service teams or relevant Third Party Supplier.

16.6 The PROVIDER will use Problem Management to reduce the number of Incidents raised to the Service Desk.

## 17 INCIDENT MANAGEMENT

17.1 The PROVIDER Incident Management System will manage Incidents, via the Service Desk, from point of receipt or discovery through to resolution.

17.2 The PROVIDER, in delivering the Incident Management System, will manage the prioritisation of Incidents to focus the right resources on the right issues. As part of the delivery of Incident Management, the PROVIDER's Support Organisation will provide effective communication with the nominated AUTHORITY's Support Staff, informing them of the occurrence and the progress of Incidents and escalating Incidents that cannot be progressed (in line with the agreed escalation approach).

17.3 As part of Incident Management, the PROVIDER will manage Major Incidents using the PROVIDER's Major Incident management process. The Major Incident management process will cover the process for raising a Major Incident, the communication frequency and the approach to resolution. The Major Incident management process will include the allocation of a Major Incident manager, a text message alert and update service and Major Incident management report production and review. Major Incidents can be called; for Severity Level 1 incidents, where resolution is not progressing as expected or Performance Measures are at risk of missing their Target Levels or in business critical emergencies. The instigation of a Major Incident will be agreed between the Parties' agreed representatives.

17.4 The Incident Management team will possess knowledge of the Infrastructure and Applications, to minimise the business impact of Incidents and ensuring resolution within the Target Levels where possible. The Incident Management team will only operate during Core Hours.

17.5 In the resolution of Incidents, the PROVIDER may need support from both its Sub-Contractors and the AUTHORITY's Third Party Suppliers. In Incidents where support from the PROVIDER's Sub-Contractors is needed, such Incidents will be managed by the PROVIDER in line with the agreed Performance Measure(s) (if any). In Incidents where support is required from the AUTHORITY's Third Party Suppliers, the PROVIDER will return the Incidents to the CHS for onwards resolution.

17.6 If a call cannot be resolved by the Service Desk and Support Organisation within the specified time (dependent on the agreed Target Levels (if any) for the associated Performance Measure), the escalation process within the Incident Management process will be followed. The escalation process will ensure that the appropriate levels of management, within both the AUTHORITY and PROVIDER organisations, are made aware of any major business / service impacting Incidents that are in danger of not being resolved within the specified time.

17.7 If the Incident is managed by the NPS ICT Team or CHS and requires the PROVIDER's expertise in working along with other suppliers, the PROVIDER will assist in restoring the service in accordance with the agreed Operational Working Agreement (OWA), which will be owned and managed by the AUTHORITY. Where no OWA exists the PROVIDER will use reasonable endeavours to support the AUTHORITY.

17.8 The PROVIDER will react to and minimise the impact of Incidents, from identification through to Resolution, via defined processes for Incident identification, triage, assignment, resolution and management.

## 18 PROBLEM MANAGEMENT

18.1 Problem Management will include the identification and diagnosis of Problems, identified through various means (including trend analysis). Incidents for which the root cause is not known will be logged by the PROVIDER's Support Organisation using the Service Management Tools, together with progress with Problem Resolution, known errors and workarounds.

18.2 The PROVIDER's Support Organisation will determine and resolve problems such that Incidents are prevented, or the impact of them is minimised via faster resolution. Where investment is required by the AUTHORITY in order to resolve a problem then the PROVIDER will use the Change Control Procedures to provide a Proposal detailing information in regards to the problem frequency, problem impact and the estimated cost of resolution.

18.3 The PROVIDER's Support Organisation will ensure that the agreed resolution to a problem is implemented through the appropriate control procedures, including Change Management and Release Management.

18.4 The Problem Management module within the Service Management Tool will provide a 'Known Error' database and will be linked to other Service Management Tool modules, including the Incident Management module, and will be available to the Service Desk to enable the effective resolution of Incidents.

## 19 REQUEST MANAGEMENT

19.1 Request Management will manage the delivery of standard service request items. These items will be published in a Product and Services Catalogue (PSC), which will be provided and maintained by the AUTHORITY's SIAM Supplier. Although the PSC will be used to capture all standard requests, only a sub-set of requests, which are relevant to the Services, will be handled by the PROVIDER. The AUTHORITY's Service Request process will ensure that the required Service Request information from End Users will be captured and the correct steps to authorise and route the request to the PROVIDER will be followed. The PROVIDER will manage the Service Requests for fulfilment and delivery.

19.2 Request Management will also provide information for service management processes including:

19.2.1 Service details, current status and any interdependencies with other Catalogue items;

19.2.2 logging requests and passing them to the appropriate service providers (internal or Third Party Suppliers);

19.2.3 fulfilment of Product and Services Catalogue requests;

19.2.4 enabling the AUTHORITY's SIAM Supplier to keep the Product and Service Catalogue up to date with devices, accessories and services;

19.2.5 responding to queries raised on orders through the Service Desk.

## 20 CHANGE MANAGEMENT AND RELEASE MANAGEMENT

20.1 The PROVIDER will implement ITIL V3 aligned formal Change and Release Management processes to promptly handle all changes and releases in line with the Service Levels.

20.2 The Change Management process will ensure that changes are recorded, evaluated, authorised, prioritised, planned, tested, implemented, documented and reviewed in a formalised and controlled manner. This will include raising (where appropriate), tracking, responding to and implementing Operational Changes through the Request for Change (RFC) form.

20.3 As part of the Change Advisory Board (CAB) approach, the PROVIDER will perform a gatekeeper function for the Services to ensure that changes are fully ready before they are deployed. Factors that will be taken into account are the degree of risk, potential impact, business benefit, complexity, timeframe and criticality. Gatekeeper measures will

include escalation of any Change Management issues to relevant members of the AUTHORITY's management team.

20.4 The AUTHORITY will notify the PROVIDER of any changes outside the PROVIDER's scope of supply but which could impact upon the provision of the Services (for example, a change to a service that interfaces to the Services provided by the PROVIDER). This notification will be made via the AUTHORITY's Joint Services Change Approval Board (JSCAB). The PROVIDER's Support Organisation will complete and submit an impact assessment in relation to any such changes and notify the JSCAB in accordance with the agreed JSCAB timeframes.

20.5 The PROVIDER will track the status of all proposed changes, and this will be jointly reviewed with the AUTHORITY at the CAB on a weekly basis to enable agreed changes to be authorised and progressed. Changes may be implemented, rejected, held over or returned for further information/discussion with the AUTHORITY as appropriate.

20.6 The PROVIDER Service Management Tool will incorporate operational change management workflows which are integrated to allow traceability, validation, handling and reporting of changes.

20.7 The PROVIDER will allocate an operational change manager who will collaborate with the AUTHORITY to achieve a holistic Change Management process including governance to minimise risk to the Services.

20.8 The PROVIDER will implement an ITILv3 aligned Release Management process, which will safeguard the integrity of the live environment and ensure that all Releases are planned, scheduled, designed, tested, packaged and deployed in a methodical and consistent manner.

## 21 MONITORING AND EVENT MANAGEMENT

21.1 Monitoring and Event Management will provide end-to-end operational management for the Applications and Infrastructure. The monitoring service will be managed through the PROVIDER's 24x7 Remote Operation Centre (ROC) which is fully integrated with the PROVIDER's Service Management Tools for end to end audit trail of Incidents and warnings. The monitoring service will:

21.1.1 monitor operational performance;

21.1.2 change events that require action into Incidents and engage the Support Organisation, where possible prior to an Incident being raised by the AUTHORITY;

21.1.3 monitor application hosting environments to ensure operation;

21.2 The monitoring service will monitor all relevant batch jobs for any alerts and error messages and respond to them appropriately.

21.3 The Service Desk will provide integrated event logging to manage Incidents and events.

21.4 The PROVIDER will schedule and configure jobs to run automatically as part of overnight, batch or online processes as required through job scheduling and in line with the Change Management process.

21.5 The Services will be monitored using the information provided by the Service Management Tools listed in Paragraph 9.

21.6 The PROVIDER will configure and utilise a suite of monitoring tools as part of the Service Management Tool. Monitoring and alerting will be closely linked with event management, providing the primary communication of operational information, warnings and exceptions to the Support Organisation. Where an exception has occurred or event information

shows that an exception will occur if no action is taken, the Service Desk will reactively (in the case of an exception) or proactively route the Incident to the appropriate Support Staff and follow any relevant escalation process.

21.7 The monitoring service will monitor and manage the operational capacity and performance of:

(a) server / storage / database / CPU;

(b) data network (connectivity),

21.8 The monitoring service will monitor system capacity and alerting should thresholds be breached.

21.9 The monitoring service and security monitoring service will be closely linked such that security monitoring is provided 24 x 7 with the Security Operation Centre monitoring security alerts during Core Hours and the Cyber Centre providing monitoring during Non–Core Hours escalating as appropriate when breaches are identified. The security monitoring will be aligned to standards listed in Schedule 7.

## 22 CAPACITY MANAGEMENT

22.1 The PROVIDER will provide Capacity Management, which will ensure that the Infrastructure is capable of meeting the evolving demands of the AUTHORITY over time. This will be conducted by the PROVIDER through analysis of current demands and forecasting, to the extent that it is appropriate to this Agreement.

22.2 The PROVIDER will undertake Capacity Management monitoring, analysis, forecasting and reporting on capacity for the Services. The PROVIDER will maintain statistics on Infrastructure demand and usage to assist the AUTHORITY in analysing future trends for the purpose of Capacity Management. The PROVIDER will, subject to agreement through the Change Control Procedures and to the extent that it is technically possible, ensure that the Infrastructure provisions are sufficient to meet the demands against any evolving requirements of the AUTHORITY.

## 23 AVAILABILITY MANAGEMENT

23.1 Availability of Services and Assets will be actively managed through Problem Management, Capacity Management and Security Management.

23.2 Subject to undertaking the Technology Refresh Projects identified in Schedule 16, the PROVIDER will be responsible for maintaining availability of the Services against the agreed Performance Measures set out in Schedule 6. The PROVIDER will take appropriate action to ensure that Incidents and problems affecting availability are resolved.

23.3 Subject to undertaking the Technology Refresh Projects identified in Schedule 16, the PROVIDER will design the Infrastructure and the Services (including processes, tools and roles) to meet the agreed Target Levels for the Performance Measures as set out in Schedule 6.

23.4 The PROVIDER will review events and Incidents that result in unavailability to investigate if design changes (other than those already planned to be undertaken as part of the Technology Refresh Projects) should be implemented to improve availability. Where such design changes would require investment from the AUTHORITY (for example where additional Hardware or Software is required) the PROVIDER will discuss with the AUTHORITY whether the changes in question should be raised through the Change Control Procedures.

23.5 The AUTHORITY will be responsible for the analysis of business/service requirements and development of any strategy that will affect the availability requirements of the existing Infrastructure. Any changes to the Agreement that are required as a result of such analysis will be handled through the Change Control Procedures.

## 24 SECURITY MANAGEMENT

24.1 The PROVIDER will implement a process to cover Information Security and compliance management and maintain an Information Security Management System (ISMS) covering all aspects of the Services as set out in Schedule 7.

## 25 CONFIGURATION MANAGEMENT

25.1 The Configuration Management Database (CMDB) is managed by the AUTHORITY's SIAM Supplier. The PROVIDER will identify, record, track, report and audit Configuration Items (CIs) in relation to the Services and provide this information to the AUTHORITY's SIAM Supplier.

25.2 The PROVIDER will protect the integrity of the Assets and CIs throughout service and/or project delivery by following the Change Management process.

25.3 The PROVIDER will track Hardware and Software components to support Software Licences and charging processes. Items recorded will include physical Assets such as Workstations, Servers and Network components and virtual Assets, such as virtual servers, firewall and network components. Small low value items, as agreed with the AUTHORITY, such as mice, keyboards and headsets will not be recorded as these will be classed as consumable items.

25.4 The PROVIDER will audit its Configuration Items at least annually to ensure that its elements of the CMDB remain accurate using a combination of the Service Management Tools and other system tools.

## 26 SERVICE REPORTING

26.1 The PROVIDER shall generate performance reports that describe how the Services are being delivered against Target Levels.

26.2 The PROVIDER shall provide a facility that enables the AUTHORITY to generate custom reports, from the Service Management information held in the repository, using a straightforward graphical user interface.

26.3 The following performance reports shall be produced and disseminated by the PROVIDER:

26.3.1 A daily performance dashboard

26.3.2 A weekly forward schedule of change detailing operational changes

26.3.3 A performance report every calendar month

26.3.4 A performance review annually, commencing 12 months after the Commencement Date.

26.4 The PROVIDER will deliver project Progress Reports that describe how significant projects and programmes relating to specific services are being delivered against plans agreed with the AUTHORITY (as agreed in the relevant project statement of work)

## 27 DISPOSAL SERVICE

27.1 The PROVIDER will ensure that any unwanted Hardware approved for disposal by the AUTHORITY is disposed of in compliance with the following standards and policies, (or the equivalent standards and policies prevailing at the time of disposal):

27.1.1 BS7799;

27.1.2 ISO9000;

27.1.3 Information Assurance Standard 5 as detailed in Schedule 7

27.1.4 The Waste from Electrical and Electronic Equipment Directive;

27.1.5 The Data Protection Act 1998;

27.1.6 The waste management and carriage licensing conditions;

27.1.7 all relevant UK and European legislation; and

27.1.8 CESG accreditation.

27.2 To dispose of an item of Hardware the AUTHORITY shall raise a Request for Service, which will be processed in accordance with the Change Control Procedures.

27.3 The PROVIDER shall, in managing the unwanted Hardware disposal process:

27.3.1 record all changes on the CMDB; and

27.3.2 provide a copy of the disposal certificate to the AUTHORITY.

27.4 When a device is no longer required at an AUTHORITY Location, the AUTHORITY shall ensure that a duly authorised representative is available to confirm any Hardware for disposal is correctly identified and collected by the PROVIDER.

## 28 ISO STANDARDS

28.1 At a corporate level, the PROVIDER has and will maintain UKAS accredited certification to the following ISO standards:

28.1.1 Quality Management System

TickITplus & ISO 9001:2008 certification for:

- Systems and Software Development & Support
- Service Management
- Programme and Project Management

This certificate applies across all of the PROVIDER's UK operations.

28.1.2 Information Security Management System

ISO 27001:2013 certification for the provision of Secure UK locations for delivery including the provision of remote operations services, IT Consultancy, IT Systems Integration and Business Process Services.
This certificate applies to most, but not all of the PROVIDER's UK operations.

28.1.3 Service Management System

ISO 20000-1:2011 certification is held by the PROVIDER's infrastructure delivery service lines for the provision of IT Service Management and infrastructure support services using the service line delivery model.

## ANNEX A – HEATMAP

1 [REDACTED]

**ANNEX B – VOLUMETRICS**

1 This Annex describes the volume of devices under support as at the Commencement Date.

| Item | Volume at Commencement Date |
|---|---|
| Thin-clients | 11,116 |
| Laptops | 2,117 |
| Desktops | 1,681 |
| Blackberry handsets | 553 |
| AT Laptops | 665 |
| Citrix Servers | 557 |
| Core NPS (CORE03) - NPS Users core applications | 327 |
| Core CRC (CORE01) - Core applications for CRC Users and CRC Exception Users | 182 |
| Flash Silo (NONCORE12) - NPS Users Flash enabled applications | 18 |
| Shared Service Silo (NONCORE13) – Used by NPS Users to access Phoenix application (time recording) | 14 |
| Citrix data collectors used by the PROVIDER to manage the farm, not accessed by Users | 6 |
| Management Servers - Used by the PROVIDER and AUTHORITY IT staff to run management consoles | 10 |

## ANNEX C – KEY PERSONNEL

1 Purpose

The purpose of this Schedule 3 Annex C (Key Personnel) is to set out the obligations of the PROVIDER in relation to specific requirements for Key Personnel.

2 List of Key Personnel

The following table lists the Key Personnel.

| Role | Named Individual |
|---|---|
| Justice Account Director | [REDACTED] |
| Client Director | [REDACTED] |
| Head of Programmes | [REDACTED] |
| Service Delivery Director | [REDACTED] |
| Commercial Manager | [REDACTED] |
| Financial Controller | [REDACTED] |
| Head of Security | [REDACTED] |

3 Key Personnel

i. The PROVIDER shall be responsible for ensuring that the list of Key Personnel is kept up-to-date and re-issued to the AUTHORITY during the Agreement upon any changes being made to the list in accordance with this Paragraph 3(i). The PROVIDER shall ensure that the Key Personnel shall remain suitably skilled and experienced to carry out their duties during the course of the Agreement.

ii. Where the PROVIDER wishes to replace any Key Personnel as permitted under this Agreement, the PROVIDER shall provide the AUTHORITY with the curriculum vitae of the proposed new Key Personnel and consult with the AUTHORITY concerning the proposed appointment. The information that the AUTHORITY may take into account when considering a change to Key Personnel proposed by the PROVIDER may include the following:

(a) Role;

(b) Qualifications;

(c) Track record /experience; and

(d) Skills and personnel qualities relevant to the Services and the role.

The AUTHORITY will also take account of the extent of the individual's contribution to the Services and the amount of the individual's working time to be spent working on the Services.

iii. If the AUTHORITY objects to the proposed appointment, the PROVIDER shall not engage such person to fill the relevant position, subject to a request for review of the objection by the PROVIDER, and shall, failing a successful review, propose to the AUTHORITY an alternative candidate.

iv. The AUTHORITY may request the PROVIDER to remove any Key Personnel in accordance with Clauses 28.7 (PROVIDER's Staff - Key Personnel) and 47 (Security) of the Terms and Conditions of the Agreement. The PROVIDER shall not be excused performance of its obligations under this Agreement as a result of compliance with any such instruction. The PROVIDER shall replace any Key Personnel that have been removed in accordance with this Paragraph and as set out in Clause 28.7 of the Terms and Conditions.

## ANNEX D – DISASTER RECOVERY

**Note:** For the avoidance of doubt, a third National Data Centre (NDC2) will exist as at the Commencement Date. The PROVIDER will be part-way through a project to Decommission this Data Centre (contracted by the AUTHORITY under the Previous Contract)_and as such will deliver no live services from this Data Centre. No Disaster Recovery will be provided for this Data Centre.

1 Introduction

i. This Annex D to Schedule 3 describes the products and processes associated with Disaster Recovery for the Services, which will be provided by the PROVIDER. Disaster Recovery will form a subset of the Business Continuity Strategy. Overall responsibility for the Business Continuity Strategy rests with the AUTHORITY.

ii. The Services will be delivered from two National Data Centres (NDC's). The Production Data Centre (NDC1) will deliver the Production Services and the Disaster Recovery Data Centre (NDC3) will provide a Disaster Recovery capability for the Production Data Centre.

iii. It should be noted that any change under the Change Control Procedures that varies the capacity or scope of the services provided from the Production Data Centre, will require an equivalent change in the capacity or scope of the services to be provided from the Disaster Recovery Data Centre. Any AUTHORITY acceptance of a proposal to change the capacity or scope of the services to be provided from the Production Data Centre which does not provide for an equivalent change in the Disaster Recovery Data Centre shall be deemed to include AUTHORITY acceptance that Disaster Recovery is not required for that change in capacity or scope of the relevant service. Proposal Documents prepared by the PROVIDER in support of the Change Control Procedures will include appropriate consideration of Disaster Recovery implications and will highlight any need for changes to the Disaster Recovery Data Centre required as a consequence of changes to the Production Data Centre.

2 Disaster Recovery Products

i. The following table lists the Disaster Recovery associated products that will be provided by the PROVIDER. Where a product is a document and a specific reference is provided then the item should be considered as a referenced document.

| No | Ref. | Title |
|---|---|---|
| 1 | OSD-042HD | Data Centre DR Design |
| 2 | OSD-298LD | Technical Recovery Plan (TRP) |
| 3 | Listed in TRP | Disaster Recovery Procedural Guides<br>- many of – listed in the Technical Recovery Plan |
| 4 | TBA | Disaster Recovery Test Strategy |
| 5 | Listed in DR Test Strategy | Disaster Recovery Test Plans – several of – to be listed in the Disaster Recovery Test Strategy |
| 6 | Listed in DR Test Strategy | Disaster Recovery Test Reports – several of – one for each invocation of a Disaster Recovery Test Plan to be listed in the Disaster Recovery Test Strategy |

3 Disaster Recovery Methodology

i. The process for Disaster Recovery will be initiated in the event of a Disaster being invoked in accordance with the agreed procedures detailed in the Technical Recovery Plan. In the event of such invocation, the PROVIDER will mobilise appropriate Personnel to restore the Services in accordance with the then current Technical Recovery Plan and Procedural Guides.

ii. The PROVIDER will produce and maintain a Technical Recovery Plan to ensure that services can be restored within an agreed time frame in the event of an interruption to the Services caused by a Major Incident or Disaster. In the event that the AUTHORITY produces a Business Continuity Strategy document then the PROVIDER will, under the Change Control Procedures, produce a Service Continuity Requirements Definition that may lead to updates in the PROVIDER'S Disaster Recovery process and associated documentation; these updates will also be made under the Change Control Procedures.

iii. The PROVIDER will implement measures that allow the Services to be restored in the event that a Disaster renders the Production Data Centre unusable.

iv. In the event of a Disaster being declared, all use of the Test Systems for testing (excluding CVE) or development purposes shall cease, and the PROVIDER shall implement the Technical Recovery Plan, in accordance with the roles and responsibilities defined therein, to undertake recovery from the Disaster.

v. Once a two Data Centre environment has been re-established (under the Change Control Procedures) that is equivalent to the original Production and Disaster Recovery Data Centres, and, subject to alternative arrangements being agreed between the AUTHORITY and the PROVIDER, the PROVIDER will restore the Test Systems to the configuration agreed in the Segment Plan. This will enable the AUTHORITY to recover a pre-Disaster Test Systems configuration and data, by copying data previously saved by the PROVIDER onto the Disaster Recovery Data Centre SAN to the restored Test Systems.

vi. The PROVIDER will operate processes that support the Service Continuity Plan and the Technical Recovery Plan. These processes will be based on an ITIL best practice framework and will be adjusted if required, under the Change Control Procedures, by the PROVIDER to suit the AUTHORITY's specific requirements.

vii. Pending production and agreement of the Service Continuity Requirements Definition, the responsibilities for declaring a Disaster and invoking the Technical Recovery Plan shall be:

(e) the PROVIDER will notify the AUTHORITY as soon as reasonably possible (using the Major Incident notification process) of a Disaster affecting the National Data Centres, and will enact the Technical Recovery Plan in order to restore the affected services and meet the Disaster Recovery requirements set out in this Schedule.

(f) the AUTHORITY will notify the PROVIDER of a Disaster affecting Locations other than the National Data Centres as soon as reasonably possible.

4 National Data Centre Disaster Recovery.

i. This section describes the various elements that make up the process for National Data Centre Disaster Recovery.

ii. Disaster Recovery Environment

(a) The PROVIDER will implement and maintain a Production Data Centre and a Disaster Recovery Data Centre.

(b) The PROVIDER will provide systems at the Disaster Recovery Data Centre that enable the continued provision of the Services from the Disaster Recovery Data Centre in the event that a Disaster is declared at the Production Data Centre.

(c) The PROVIDER will, with assistance from the AUTHORITY, review its Disaster Recovery Data Centre systems and present the findings in a report to the AUTHORITY annually with the first such report to be provided within 6 Months of the Commencement Date. The PROVIDER will, if required by the AUTHORITY, adjust the design of the Disaster Recovery Data Centre systems under the Change Control Procedures so that the Disaster Recovery solution remains Value for Money for the AUTHORITY.

(d) The Disaster Recovery Data Centre will comply with the requirements for Hosting Facilities as detailed in Schedule 15 (Environmental Conditions).

(e) Hardware for testing and development Segments will be drawn from that provided for Disaster Recovery, and will consist of Servers and part of the SAN located at the Disaster Recovery Data Centre. The capacity of the Segments is limited to that provided by these Disaster Recovery systems and Central File Storage.

5 Disaster Recovery Processes

i. The AUTHORITY will produce and share with the PROVIDER a Business Continuity Strategy and maintain this throughout the Term.

ii. The PROVIDER will work with the AUTHORITY to produce, within three (3) Months of release or re-release of the Business Continuity Strategy, the Service Continuity Requirements Definition that will support that Business Continuity Strategy. Implementation of any Change to the Services and/or Infrastructure required to support the Service Continuity Requirements Definition will be carried out under the Change Control Procedures

iii. The PROVIDER will work with the AUTHORITY to develop and agree, within three (3) Months of acceptance of the Service Continuity Requirements Definition, a revised Service Continuity Plan and Technical Recovery Plan that meets the requirements of the Business Continuity Strategy. Implementation of any Change to the Services and/or Infrastructure required to support these Plans will be carried out under the Change Control Procedures.

iv. Pending production and agreement of the Service Continuity Requirements Definition the PROVIDER's Service Continuity Plan will include, without limitation:

(a) an agreed escalation structure which will be capable of dealing with crisis management in the event of a Disaster;

(b) details of provision of a Disaster Recovery Data Centre to enable recovery from a Disaster affecting the Production Data Centre;

(c) details of offsite backup up of primary data storage at the Production Data Centre;

(d) details of how WAN Connections at the National Data Centres are configured so that the loss of any Network connection shall not result in a total loss of connectivity.

v. The Disaster Recovery Data Centre will also be used for non-production services to undertake Testing and Development as further specified in this Schedule 3.

vi. The systems at the Disaster Recovery Data Centre will be managed by Server management software that will enable these systems to be rapidly reconfigured, supporting their use for the multiple roles envisaged for the Disaster Recovery Data Centre.

vii. The PROVIDER will implement and Maintain back-up services at the Production Data Centre and the Disaster Recovery Data Centre to ensure that systems and data can be recovered in the timescales specified within Paragraph 5(viii) of this Annex in the event of a Disaster.

viii. The PROVIDER will develop a Technical Recovery Plan to ensure the prompt restoration of the Services in the event of a Disaster. The Technical Recovery Plan will define processes to restore the Services as follows:

(a) Critical IT Services (as defined in Paragraph 5(x) below) are to be restored within 24 hours of the invocation of the Disaster Recovery process; and

(b) the remaining IT services that are to be recovered are to be restored within 5 days of the invocation of the Disaster Recovery process.

ix. The Technical Recovery Plan will also define which IT services are not to be recovered under the Technical Recovery Plan.

x. The following table details all services that are deemed as Critical IT Services and which will be restored in accordance with the recovery time objective as defined in Paragraph 5(viii)(a) above. Note that these services will not necessarily be restored in the order indicated.

| **Service** | **Components** |
|---|---|
| Radia | All |
| Backup | All |
| Citrix | All |
| Print | All |
| Domino Mail | All |
| Domino Applications | All |
| System Logging | All |
| File Services | Personal and Group Shares |
| Shared SQL | For ePO |
| ePO Anti Virus | All |
| Tools Monitoring | All |
| Active Directory | All |
| NDC Network Services | ACS |
| BAU Recovery Service | Server Break-Fix |
| HP SIM | All |
| NDC Storage Services | Management functions |
| My Documents | The most recent version of each document |

xi. The following table details all services that are deemed as non-critical and which will be restored in accordance with the recovery time objective as defined in Paragraph 5(viii)(b) above. Note that these services will not necessarily be restored in the order indicated.

| **Service** | **Components** |
|---|---|
| File Services | Quotas, VSS and Defragmenter |
| Wyse Device manager | All |
| Shared SQL | For Wyse Device Manager, for File Quotas, for RADIA |
| Sanctuary | All |
| Tools | Reporting |
| NDC Network Services | CiscoWorks |
| BAU recovery Services | AD-hoc restore requests |
| Introduce / Replace Client Services | Laptops, Desktops, Wyse Terminals |

xii. The following services will not be restored (as per Paragraph 5(ix) above) as part of Disaster Recovery.

| Service | Components |
|---|---|
| My Documents | Only the most recent versions will be restored not any other versions |
| DVE | All components of the Development and Validation Environment |

xiii. The PROVIDER will restore services in line with the Technical Recovery Plan

xiv. The operational environment for the Business Support Applications will be re-established in line with the Technical Recovery Plan in the event of a Disaster.

xv. Application services will be restored according to the Technical Recovery Plan in the event of a Disaster.

xvi. Service Desk services will be restored in line with the Technical Recovery Plan in the event of a Disaster.

xvii. The PROVIDER will utilise appropriate tools to support Service Continuity Management which shall include:

(a) reference to the AUTHORITY's business recovery objectives;

(b) undertaking risk assessments, vulnerability and threat analyses;

(c) identifying options for achieving business recovery objectives;

(d) planning service continuity activities;

(e) determining the technology, organisation and process decomposition and single point of failure analysis; and

(f) testing Service Continuity Plans.

6 Disaster Recovery Organisation

i. The PROVIDER will be responsible for the continuity of service of the System and Services on a day-to-day basis and planning for corrective action in the event of a Major Incident or Disaster.

ii. The PROVIDER will make available, through the Change Control Procedures, business and service continuity planning, training, support and consultancy services, as requested by the AUTHORITY.

## ANNEX E – DESCRIPTION OF OPERATIONAL RISK

1 Annex E to this Schedule 3 (file name "New OMNI Sch 3 Annex E – Service and security risks list v1.4 11122016") has been reproduced on the compact disc (affixed below) which is labelled as "PICTS Contract Documents" and has been signed for and on behalf of the PROVIDER and the AUTHORITY and dated with the date of this Agreement.

2 Annex E provides an overview of the operational risks present as at the Commencement Date and the proposed mitigation within the Technology Refresh programme. As noted within Annex A not all operational risks are addressed by the Technology Refresh programme.

3 This Annex E should be read in conjunction with:

i. Annex A - Heatmap

ii. PROVIDER / AUTHORITY joint service risk/issue register

**[REDACTED]**

## ANNEX F - SOFTWARE AND SUPPORT

1 The PROVIDER's delivery of the Services requires that a number of Software licences and Software and Hardware maintenance and support agreements shall be in place. Where the PROVIDER provides these Software licences and Software and Hardware maintenance and support agreements they are listed in Table A or B of this Annex. Those paid for under the Core Service Charge are listed in Table A. Those renewed via the Support Renewal Charge line in the Charges Model are listed in Table B.

2 Any additional such agreements that are required to enable delivery of the Services, that are not listed within this Annex F will be managed through the Change Control Procedures and shall be to the AUTHORITY's account.

3 PROVIDER AGREEMENT RENEWALS

i. Table A below sets out those Software licences and Software and Hardware support and maintenance agreements where the PROVIDER will procure and pay for the renewals on behalf of the AUTHORITY as part of the Core Service Charge as set-out in Schedule 5.

ii. Table B below sets out those Software licences and Software and Hardware support and maintenance agreements where the PROVIDER will procure and pay for the renewals on behalf of the AUTHORITY during the Term of the Agreement. These agreements will be reviewed and renewed annually unless otherwise agreed by the Parties. The scope and quantities related to such agreements will be reviewed annually by the 1st December each Contract Year and the associated Charges will be confirmed to the AUTHORITY following each such review. Any changes to the estimated Charges, as set out within Schedule 5, will be managed through the Change Control Procedures.

4 AUTHORITY AGREEMENT RENEWALS

i. Table C below sets out those Software licences and Software and Hardware support and maintenance agreements where the AUTHORITY has agreed to take on the responsibility to procure and pay for such agreements directly. The PROVIDER acknowledges that the AUTHORITY will continue to renew these agreements directly rather than through the PROVIDER (unless the Parties agree otherwise through the Change Control Procedures).

ii. Where the AUTHORITY has taken on responsibility to procure and pay for such agreements directly, then the AUTHORITY shall provide the appropriate documentation (including licence keys, agreement reference numbers and full details of how support is to be obtained from the product vendor as applicable) and any access codes or permissions to allow the PROVIDER to access the support and maintenance services delivered through those agreements.

iii. The AUTHORITY responsibility set out in paragraph 4(ii) above shall be deemed to be included within the definition of AUTHORITY Responsibilities for the purposes of interpretation of Clause 2.2 of the Agreement.

**Table A – PROVIDER AGREEMENT RENEWALS PROVIDER VIA CORE SERVICE CHARGE**

| Supplier Name | Description of Service | Renewal date |
|---|---|---|
| Avnet | HP Hardware & Software support | 31st December |
| BT | BT – Cardiff Data Centre | 31st December |
| Geotronics | Geotronic LAN equipment maintenance | 31st December |
| Com-Com | HP Service desk and HP Openview | 31st December |
| Expisoft | SecureOffice software 3rd party support | 31st December |

| Supplier Name | Description of Service | Renewal date |
|---|---|---|
| KN3 Ltd | KN3 Build Manager | 31st December |
| Blancco UK | Blanco - Secure Hard Drive data erasure software | 31st December |

**Table B – PROVIDER AGREEMENT RENEWALS PROVIDER VIA THIRD PARTY AGREEMENT CHARGE**

| Supplier Name | Description of Service | Renewal date |
|---|---|---|
| Avnet | Hardware Maintenance Services – Protectier<br>IBM On-site repair for Virtual Tape Library (VTL) related systems | 31st December |
| Avnet | Software support Services – Protectier for Virtual Tape library (VTL) related systems | 15th December |
| Arrow | NTP/QFS - Quota and File Manager software, support and maintenance renewal | 31st December |
| ASM Technologies | Radia Software support (PSL Radia Server Mgmt Svr SW E-LTU) | 31st December |
| Avnet | NetApp Filer support for NPS National Share drives | 31st December |

**Table C – AUTHORITY PROVIDED AGREEMENT RENEWALS**

| Supplier Name | Description of Service |
|---|---|
| Radia | Radia Client Mgmt. plus CAE management software (MoJ ref 441) |
| Symantec | Symantec Netbackup and Backup Exec & Hyper V |
| Symantec | Symantec Netbackup Client Application and Enterprise Client |
| VMware | Enterprise Agreement for vSphere and vCentre |
| IWG | M86 Internet Web Gateway Subscriptions and Hardware Warranty and software support for production and test kit |
| McAfee | McAfee Antivirus support and maintenance including for NetApp |
| Sophos | Sophos Anti virus - Support and Maintenance for Windows and UNIX |
| MIMESweeper | MIMESweeper - Maintenance Renewal for MIMESweeper, licenses, Support and maintenance |
| Lumension | Lumension encryption |

| Supplier Name | Description of Service |
|---|---|
| Transputec | Clive House wireless network |
| Domino | Domino Server and Lotus Notes |
| SAP | SAP Business Objects |
| Oracle | Oracle Enterprise licencing |
| Citrix | Citrix XenApp and Netscaler licences |
| Azlan | Enterprise Agreement for vSphere Standard/ vCenter Server Standard/ vSphere Enterprise/ vSphere Standard/ vCenter Server Standard |
| Trustmarque | Eventsentry licences |
| Microsoft | All required Microsoft licences including Active Directory, Microsoft Server, Microsoft O/S, Microsoft Office |